CAMPUS
DE EXCELENCIA
INTERNACIONAL

Máster Universitario en Ingeniería Informática

Universidad Politécnica de Madrid

Facultad de Informática

TESIS FIN DE MASTER

Guía para la Implementación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores Prácticas

Autor: Kevin Edgardo Ducón Pardey

Director: José Domingo Carrillo Verdún

DEDICATORIA

A mi Madre de quien he aprendido que las cosas con perseverancia, esfuerzo y trabajo se consiguen satisfactoriamente; a mi Padre que me hizo apasionar por el mundo de la informática y por la lucha incansable por lograr los proyectos que nos proponemos; a mi familia que nunca me ha dejado solo y ha estado ahí todo el tiempo, gracias por su compañía, su comprensión y por todos los detalles mientras he estado lejos, quiero que esto sea un motivo de orgullo e inspiración para ustedes.

A Paito, mi compañera de lucha, mi amiga, mi amor, que no solo fue tolerante y contribuyó a la consecución de este trabajo, sino que me dio más de 8.000 de razones para darle las gracias. Espero que esta experiencia contribuya a nuestro proyecto de vida y te aporte personal y profesionalmente.

A mis amigos, aquellos que no les importó la distancia, y que siempre estuvieron a mi lado, con una llamada, un mensaje, siempre con esas palabras de aliento y con ese deseo de poder compartir de nuevo.

AGRADECIMIENTOS

Quisiera agradecer de manera amplia al Profesor Dr. José Carrillo Verdún, por su tutoría durante este trabajo, por su paciencia, esfuerzo y sobre todo por el apoyo incondicional durante la elaboración del proyecto. También por el amplio conocimiento que ha transmitido a través de sus cursos y que fue fundamental para tomar mi decisión y optar por trabajar y profundizar en estas áreas de conocimiento. También agradecer a su equipo de trabajo en las diversas asignaturas que dirige.

A los compañeros de Máster, porque durante estos dos años he tenido no solo la oportunidad de compartir académicamente con algunos, haber aprendido de manera significativa y realizar muy buenos trabajos, sino que de manera extracurricular hemos creado lazos fraternales dignos de admirar y que espero perduren después de este lapso.

Agradecer a los profesores del Máster universitario, por compartir su conocimiento el cual esperaré poner en práctica durante mi vida profesional.

Agradecer de manera especial a Colfuturo porque permitió que mi sueño de estudiar fuera del país se mantuviera, a pesar de las dificultades que han generado las reformas.

A las personas que directa o indirectamente me han ayudado a que salga adelante este proyecto de estudio y como producto, este Trabajo Fin de Máster.

RESUMEN

El papel de la tecnología en las organizaciones es mucho más relevante, lo que en su momento era innovación, hoy por hoy es un soporte a varias funciones del negocio y la automatización de procedimientos vitales para el alcance de la misión de la organización. Esto se debe a que la tecnología ha transformado y sigue transformando los procesos de negocio que soportan los servicios y ayudan a conseguir los objetivos y la misión de la organización.

Un activo tecnológico cada vez más importante para el buen funcionamiento de las organizaciones es el software. Dada la complejidad de los procesos en los que interviene, cada vez su importancia es más crítica y los defectos en su fabricación son el objetivo fundamental de los delincuentes y uno de los mayores riesgos para las organizaciones. Hay que considerar que no todas las organizaciones construyen o diseñan software, algunas veces lo hace un tercero, lo adquieren a otra organización, o puede ser contratado como SaaS. Pero durante el proceso de construcción, adquisición o contrato ¿Se han tenido en cuenta las amenazas y nuevos ambientes de riesgos a los que se expone la organización? ¿Se ha considerado la relación entre el software y los servicios de alto valor de la organización? ¿Existen planes de seguridad y continuidad sobre los servicios?

Tendremos que establecer estrategias de Protección y Sostenimiento que garanticen que el software tendrá la máxima disponibilidad posible para funcionar posteriormente a un evento de interrupción o estrés –así sea en condiciones degradadas– evitando paradas en los servicios, lo que llamamos resiliencia operacional. Esto será una estrategia desde la dirección hasta la operación, asegurando que durante todo el ciclo de vida del software y durante su administración se sigan los procedimientos, planes, metodologías y técnicas necesarias que aseguren que el software es resiliente y que cumple con los requisitos de resiliencia a nivel operacional.

Esta guía busca orientar a la alta gerencia, a los mandos medios y a nivel profesional en las prácticas que implican asegurar la resiliencia operacional del software y la resiliencia del software como tal, y está basada en marcos metodológicos y de control, estándares, modelos y mejores prácticas actuales que soportan los procesos que implica la consideración de la resiliencia operacional sobre el software. Del mismo modo se considerarán los tipos de software y las prácticas a implantar para cada uno de ellos, orientado al proceso que implica y a las responsabilidades que demandan.

ABSTRACT

The role of technology in organizations is much more important, what at some time was innovation, now is support of multiple business functions and the automation of vital procedures in order to reach organization's mission. This is because to Technology has transformed and still transforming business processes that supports services, and at the same time helps to achieve the organization's goals and mission.

An increasingly important technological asset for the best perform in organizations is software. Given the complexity of the processes which software is involved, its importance is becoming more critical and defects during development are the fundamental objective of attackers and one of the greatest risks for organizations. Consider not all organizations build or design software sometimes it does a third party; or they acquire it to another organization, or could be contracted as a SaaS. But during the process of development, acquisition or contract, Has it taken into account the threats and new risks environments which the organization is exposed? Has it considered the relationship between the software and organization's high-value services? Are there security and continuity plans for services?

We will have to develop protect and sustain strategies to ensure that software will have the highest possible availability to work after a disruption or stress event –whether in degraded conditions– avoiding service stops, what we call operational resilience. This will be a strategy from management to operation, ensuring that throughout the software life cycle and during administration, procedures, plans, methodologies and techniques are followed, to ensure that the software is resilient and met operational-level resilience requirements.

This guide seeks to guide managers and professionals in practices involving ensure software operational resilience and software resilience as such, and it's based on current methodological and control frameworks, standards, models and best practices that support the processes involved in the consideration of software operational resilience. Similarly it will consider software types, and practices to implement for each one, including processes and demanding responsibilities.

TABLA DE CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

GLOSARIO

Activo: Cualquier cosa que tenga valor para la organización. [ISO/IEC 13335-1:2004]

Acuerdo de Nivel de Servicio SLA: Acuerdo escrito entre un proveedor del servicio y un cliente en el que se documentan los servicios y los niveles de servicio acordados. [ISO/IEC 20000:2005]

Amenaza: Probabilidad de ocurrencia de un evento de cierta magnitud que puede comprometer un activo (tangible o intangible) en la organización.

Ataque: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera. [ISO/IEC 18043:2006]

Continuidad del Negocio: Capacidad de una organización para continuar entregando productos o servicios a unos niveles predefinidos aceptables después de un incidente de interrupción. [ISO 22301:2012]

Cloud Computing: Es un modelo que permite de manera conveniente y por demanda acceso a red a un conjunto compartido de recursos informáticos configurables (p. ej. redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser aprovisionados y entregados de manera rápidamente con un mínimo esfuerzo de gestión o de interacción con el proveedor de servicios. [NIST 800-145]

Disponibilidad: Capacidad de un componente o un servicio para realizar la función requerida en un instante determinado o a lo largo de un periodo de tiempo determinado. [ISO/IEC 20000:2005]

Entrega: Conjunto de elementos de configuración, nuevos o modificados, que están probados y se introducen de forma conjunta en el entorno real. [ISO/IEC 20000:2005]

Gestión de Riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. [ISO/IEC 27001:2005]

Gestión de Servicios: Gestión de los servicios para cumplir con los requisitos del negocio. [ISO/IEC 20000:2005]

Gestión de TI: Decide como la TI debe utilizarse para conseguir un uso eficaz y eficiente de los recursos y ayudar a alcanzar los objetivos del negocio. [CARR12] Sistema de controles y procesos requeridos para la consecución los objetivos estratégicos establecidos por el cuerpo de gobierno. La gestión está sujeta a las guía de las políticas y monitorización establecidas por la gobernanza corporativa. [ISO/IEC 38500:2008]

Gobernanza Corporativa: Forma en que las empresas se organizan, son dirigidas y controladas. [Asociación Española de Contabilidad y Administración de Empresas]

Gobernanza Corporativa de TI: el sistema mediante el cual la TI es dirigida y controlada. [CARR12]

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [ISO/IEC 27001:2005]

Plan de Continuidad del Negocio BCP: Procedimientos documentados que guían a las organizaciones para responder, recuperarse, reanudar y restaurar a un nivel predefinido de operación después de la interrupción. [ISO 22301:2012]

Resiliencia: Propiedad física de un material cuando puede volver a su posición o forma original después de una deformación que no excede su límite elástico. [WordNet]

Resiliencia Operacional: Resiliencia operacional es la propiedad emergente de una organización que puede continuar llevando a cabo su misión después de una interrupción que no excede su límite operacional. [CRMM10]

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización [Adaptada de la definición 2.19 de ISO/IEC 13335-1:2004]. Se consideran cuatro tipos de riesgo generalmente aceptados Riesgo Operacional, Riesgos de Peligros (Naturales), Financieros y Estratégicos. [CEBU11]

Riesgo Residual: Riesgo remanente después del tratamiento de riesgos. [ISO/IEC 27001:2005]

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad [ISO 17799:2005]. Confianza en que los sistemas de información están libres y exentos de todo peligro o daño aceptables. [UNE 71504:2008]

Seguridad Informática: Es la seguridad de la información aplicada a la tecnología.

Software como servicio (Software as a Service SaaS): Modelo de servicio de Cloud Computing. Capacidad ofrecida al consumidor para usar las aplicaciones del proveedor que se ejecutan en una infraestructura de nube. Las aplicaciones son accesibles desde diferentes dispositivos cliente a través de una interfaz de cliente ligero como un navegador web (por ejemplo, el correo electrónico basado en la web). El consumidor no administra ni controla la infraestructura subyacente cloud incluyendo la red, servidores, sistemas operativos, almacenamiento e inclusive capacidades individuales de la aplicación, con la posible excepción de los ajustes limitadas de configuración de la aplicación específica de usuario. [NIST 800-145]

Software Resiliente: Software con la habilidad para recuperarse y ajustarse a sí mismo en situaciones de interrupción o estrés logrando ejecutar la tarea para la cuál ha sido diseñado, apoyando los servicios de la organización.

Vulnerabilidad: Debilidad de uno o un grupo de activos que puede ser explotada por una o varias amenazas. [ISO/IEC 1335-1:2004]

1. INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

El papel de la tecnología en las organizaciones es mucho más relevante Lo que en su momento era innovación, hoy por hoy es soporte a varias funciones del negocio, la automatización de procesos y la transformación del negocio, lo que hace a la tecnología vital para alcanzar la misión de la organización. Con este crecimiento de TI en la empresa fue necesario gestionarla, sin embargo con el crecimiento de la organización, la TI podía funcionar pero no estaba orientada a apoyar la estrategia del negocio ni integrada en los procesos del mismo, siendo su uso un tanto errático, sin un rumbo claro en su dirección y se empezó a hablar de Gobierno de TI.

Al establecer un Gobierno de TI alineado con la Gobernanza Corporativa, no solo ofrece las ventajas de alinear las prácticas de TI a la estrategia, los objetivos y la misión de la organización, al mismo tiempo ofrece una visión holística, donde tendremos un panorama claro entre los servicios y las Tecnologías de la Información. Bajo el Gobierno de TI, se establece la gestión de TI, que se encargará de la función de TI, pero que también buscará asegurar una óptima gestión de servicios de TI. De manera paralela, surge en la organización la gestión de la seguridad de la información, con el objetivo de proteger la información – y a la vez implica la implantación de medidas de seguridad informática que brinda una protección a la organización a nivel de TI–, y la gestión de la continuidad de negocio que ayuda a las organizaciones a sobreponerse a amenazas que puedan interferir su operación normal.

De acuerdo a un estudio realizado por Gartner[1], en la seguridad de IT sólo se gasta entre el 2% y el 7% del presupuesto total de IT, del cual la mayoría se gasta en la seguridad de las redes. En contraste, indican que el 75% de las amenazas de seguridad se deben a defectos en el software.

En un principio, las organizaciones adquirían su paquete software, luego demandaron software a la medida, por lo cual algunas organizaciones probaron con equipos internos de

[1] [http://www.gartner.com/technology/metrics/]

desarrollo y otras simplemente contrataban a un tercero, pero ahora con el auge del Cloud Computing, el Software como Servicio SaaS es una opción rentable para la organización. El producto puede ser el mismo y suplir la misma funcionalidad, pero las responsabilidades, los procesos, las vulnerabilidades, el soporte y en general la gestión sobre el software cambia. Los defectos en el software se deben en gran parte a fallas en el proceso, en el ciclo de vida, en algunos casos importa más el precio o el tiempo de la entrega que la calidad, y esto incluye que no se tengan en cuenta los requisitos de seguridad desde el principio.

El software, considerado como un activo tecnológico, suele soportar servicios de alto valor para la organización, y por esto será un activo al cuál se le valorará en cuanto al riesgo que representa su interrupción para el alcance de la misión de los servicios. Como se decía anteriormente, las organizaciones día a día soportan más servicios operativos en la tecnología, algo que preocupa en cuanto las amenazas a las que a diario se expone el software. Amenazas técnicas de malware en las aplicaciones, intrusiones, vulnerabilidades en el proceso de construcción aprovechadas, entre otros.

Pero no sólo existen amenazas a nivel técnico, el auge de los crackers, los excesivos privilegios internos, acceso de terceras partes, ingeniería social y negligencia interna, e inclusive el riesgo que el proyecto no se lleve a cabo son otras causas igual de comprometedoras. Del mismo modo situaciones impensables e improbables (*Black Swan*) que se materializan, ataques terroristas, fuerzas de la naturaleza, en fin. Las condiciones actuales hacen que la gestión de riesgos sea estratégica para las organizaciones en diversos escenarios, pero a la hora de la verdad esto representa un alto costo para la organización y queda la duda, ¿este marco de gestión de riesgos es suficiente para garantizar que los servicios sigan operativos después de que un riesgo se materializa?

Tendremos que establecer estrategias de Protección y Sostenimiento que garanticen que el software tendrá la máxima disponibilidad posible para funcionar posteriormente a un evento de interrupción o estrés –así sea en condiciones degradadas– evitando paradas de servicio, lo que llamamos resiliencia operacional. Esto será una estrategia desde la dirección hasta la operación, asegurando que durante todo el ciclo de vida del software y durante su administración se sigan los procedimientos, planes, metodologías y técnicas necesarias que aseguren que el software es resiliente y que cumple con los requisitos de resiliencia a nivel operacional.

La resiliencia es una realidad, y un compromiso en las organizaciones debido a una preocupación principal, el ciberterrorismo. En el *World Economic Forum* del año 2011 se inició un proyecto alineado con la ciberseguridad para identificar los riesgos a nivel global incrementados por la interconectividad de personas, procesos y objetos, y con esto vulnerabilidad de robo o pérdida de activos. En este proyecto, el resultado es una iniciativa para la ciberresiliencia, y aunque esta es general, no cabe duda que el software, como uno de los puntos más vulnerables, tendrá que ser evaluado.

Algunos proyectos de software ya implican el concepto de Software seguro, que es aplicar mejores prácticas de seguridad para el diseño, construcción y pruebas. Este software está "blindado" a vulnerabilidades conocidas y probadas, y es una práctica que requiere de un alto conocimiento, sin embargo hay una brecha entre la ingeniería de software y la seguridad, y no un proceso colaborativo, pues los requisitos de seguridad no pertenecen a la funcionalidad y se van descartando, no hay una cultura de seguridad en el desarrollo, o simplemente se considera "muy costoso".

¿Es suficiente para las organizaciones realizar prácticas de desarrollo de seguro para garantizar la resiliencia del software que soporta los servicios de la organización? Contribuye en gran parte, sin embargo las relaciones que tenga el software con otros activos como tal y los servicios que llegue a soportar, implican que los requisitos de resiliencia del software, enmarcados dentro de la resiliencia operacional, nos haga plantear medidas más allá de las medidas técnicas, e implantar una cultura para la resiliencia del software y de su implicación con los servicios.

Esta guía busca orientar a la alta gerencia, a los mandos medios y a nivel profesional en las prácticas que implican asegurar la resiliencia operacional del software y la resiliencia del software como tal. Esta guía está basada en marcos metodológicos y de control, estándares, modelos y mejores prácticas actuales que soportan los procesos que implica la consideración de la resiliencia operacional sobre el software. Del mismo modo se considerarán los tipos de software y las prácticas para cada uno orientado al proceso que implica y a las responsabilidades que demandan.

1.2 Objetivos

1.2.1 General

Diseñar una guía de mejores prácticas para la implementación de la resiliencia en el software desde el punto de vista de las organizaciones, tanto para la construcción, adquisición o contrato de software, con base a estándares y modelos que aporten a la implementación de la resiliencia operacional, enmarcada por un modelo de gestión de TI y bajo los principios de gestión de la seguridad, gestión de servicios de TI y continuidad del negocio.

1.2.2 Específicos

- Identificar y analizar la importancia de la Gobernanza de TI en las organizaciones desde el punto de vista de la resiliencia operacional.

- Utilizar como referencia diferentes estándares y marcos relacionados con la Seguridad de la Información, Gestión de Tecnología, Gestión de Servicios de TI, Continuidad del Negocio, que pueden aportar de forma importante al entendimiento del concepto de resiliencia en las organizaciones.

- Considerar el estado del arte en cuanto a resiliencia operacional y resiliencia software e investigar modelos que aporten a su puesta en marcha.

- Analizar la importancia de la gestión de riesgos en la resiliencia operacional, y específicamente en la resiliencia software.

- Definir los conceptos de Software Assurance (SwA) y calidad de software, y conocer su papel dentro de la resiliencia software.

- Con base a los hallazgos, plantear una guía de mejores prácticas a llevar a cabo si se desea tener en cuenta Resiliencia Software en las organizaciones.

- Identificar los beneficios y la importancia del diseño de software resiliente para las organizaciones.

- Analizar los beneficios de aplicar resiliencia software en las organizaciones, e identificar los posibles usuarios de la guía en la organización.

- Establecer las aplicaciones que tiene la resiliencia software en la situación de mercado de tecnologías de la información actual.

- Plantear líneas de investigación complementarias que garanticen la continuidad del proyecto y que contribuyan a la generación de nuevos conocimientos.

2. ESTADO DEL ARTE

2.1 Gobernanza Corporativa de la Organización

Según la Asociación Española de Contabilidad y Administración de Empresas AECA, se entiende por gobernanza corporativa "la forma en que las empresas se organizan, son dirigidas y controladas". Se requiere que las empresas establezcan una dirección estratégica de sus activos, que esté alineada con los objetivos de negocio y le ayuden a conseguir con éxito la misión establecida. Este concepto adicionalmente ha tomado importancia debido a la influencia de las nuevas economías, la responsabilidad social corporativa y el beneficio de todos los grupos de interés, y ha hecho que las organizaciones cotizadas se preocupen por el establecimiento de códigos de "buen gobierno".

El Código Unificado de buen gobierno para sociedades cotizadas, incorpora recomendaciones, de carácter voluntario, sobre buen gobierno de sociedades con acciones cotizadas en Bolsa. Dentro de este código se destaca la creación de comisiones, una comisión delegada y una de supervisión y control, constituida por los comités de auditoría, nombramiento y retribuciones. El Comité de Auditoria debe velar por el buen funcionamiento de los sistemas de información y control interno y por la política de control y gestión de riesgo. [CARR12]

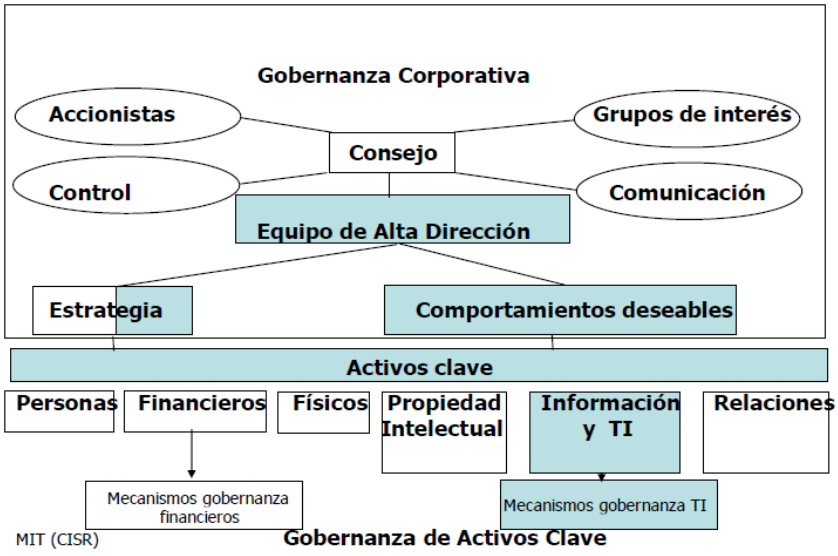

Figura 1. Gobernanza y Activos Clave [MIT-CISR]

Eso indica que para las organizaciones, en cuanto a Gobernanza de Negocio, es importante tener un mecanismo de gobernanza que haga una gestión eficaz de los recursos de TI, que realice el control de TI y que demuestre que se cumplen los requisitos corporativos en cuanto a Sistemas de Información y Tecnología de la Información. Este mecanismo es la Gobernanza Corporativa de TI.

2.2 Gobernanza Corporativa de TI

La gobernanza de TI "Es el sistema mediante el cual la TI es dirigida y controlada. La estructura de Gobernanza Corporativa aplicada al activo TI especifica la distribución de derechos y responsabilidades entre los diferentes participantes, tales como el consejo, negocio y directivos de TI. Con ello, también se proporciona la estructura mediante la cual se definen los objetivos de TI, los medios para alcanzar dichos objetivos y seguir su rendimiento". [CARR12].

En la actualidad las organizaciones delegan una gran responsabilidad al departamento de TI, y esto es debido a que con el tiempo TI es parte importante de un servicio interno o externo de la empresa, bien sea preservar la disponibilidad de la aplicación contable de la organización, prestar un servicio de comercio electrónico a través de una web o bien transformando el negocio. Para la organización es importante que las operaciones de TI mantengan una calidad determinada según la estrategia definida por el máximo órgano de gobierno de la organización para la TI, o que estén alineadas con los objetivos de la organización. En general, TI es una parte fundamental que tiene ser controlada y dirigida, pero que no sólo es responsabilidad de un departamento sino que debe ser consecuente con la gobernanza definida por la organización, debido a que de TI dependerán muchos servicios a nivel interno y externo, y "Esta mayor dependencia de TI implica una amplia vulnerabilidad que está presente de forma inherente en los entornos de TI." [CARR12]. Por esta razón, la gobernanza de TI tiene que establecer estrategias que le permita manejar los riesgos de sus operaciones de manera adecuada, pues es evidente que a partir de la actividad de TI se tendrán que definir nuevas estrategias, que pues la TI se convierte no solo en un factor de éxito sino también de supervivencia y prosperidad, así como una oportunidad de diferenciación y de alcanzar ventajas competitivas. [CARR12]

Para realizar una gobernanza de TI que cumpla las expectativas de la Gobernanza Corporativa, es necesario fijarse en las mejores prácticas, y por esto se recomienda el uso de marcos de gobernanza como UNE/ISO/IEC 38500, Calder-Moir., CobiT5 y varios más.

Tomaremos como referencia la norma ISO/IEC 38500. La norma ISO/IEC 38500 pretende guiar a la dirección (Dimensión de Gobernanza Corporativa), en el uso eficaz, eficiente y aceptable de TI en la organización. Es aplicable a cualquier tipo de organización. "Se aplica a la gobernanza de los recursos, computadoras y otros, que se utilicen para proporcionar servicios de información y comunicaciones en una organización. Estos recursos pueden ser proporcionados por especialistas de TI, de dentro de la organización o de proveedores de servicios externos o por unidades de negocio dentro de la organización." [CARR12].

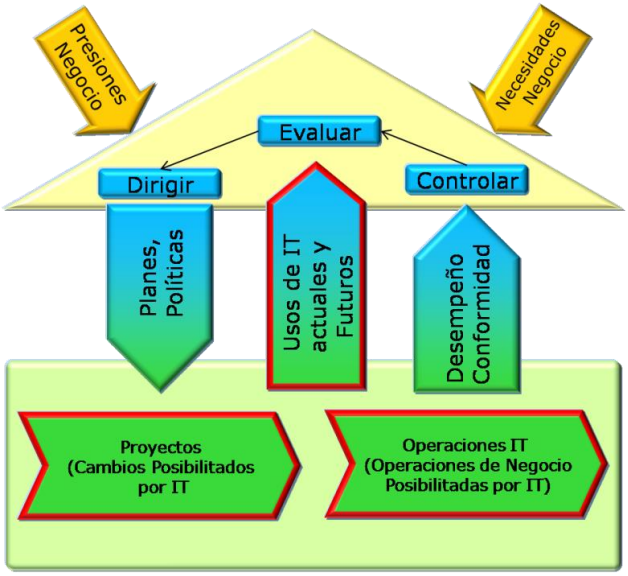

Figura 2. ISO/IEC 38500 - Modelo para Gobernanza Corporativa de TI [ISO38500]

El uso de la norma UNE/ISO/IEC 38500 es vital para las organizaciones, como una evaluación objetiva de la aplicación de la gobernanza corporativa a la TI, un mecanismo para la verificación del cumplimiento con la legislación vigente, una manera eficaz de implementar y operar los recursos de TI, un mecanismo de gestión de la continuidad del negocio, alineamiento de TI con objetivos del negocio, establecimiento de responsabilidades dentro de la consecución de objetivos del negocio a través de TI, una manera de verificar que se logran los objetivos de TI de la organización, asignación eficiente de recursos de TI, innovación en servicios y operaciones, mejora en la relaciones con stakeholders, reducción de costes de TI, beneficios concretos de las inversiones de TI, guiar a los directores a

identificar las áreas de riesgo en la implantación y uso de las TI, minimizar los riesgos de inconformidad (legal, contractual).

2.3 Gestión de TI

La Gestión de TI "decide como la TI debe utilizarse para conseguir un uso eficaz y eficiente de los recursos y ayudar a alcanzar los objetivos del negocio. Debe ser desarrollada por toda la organización TI y por las unidades de negocio. La responsabilidad de la Gestión de TI es de la función de TI" [CARR12].

La Gobernanza corporativa de TI y la Gestión de TI son conceptos distintos, pero están estrechamente relacionadas pues la norma UNE/ISO 38500 define el concepto de Gestión como: "El sistema de controles y procesos requeridos para la consecución los objetivos estratégicos establecidos por el cuerpo de gobierno. La gestión está sujeta a la guía de las políticas y monitorización establecidas por la gobernanza corporativa." [ISO38500]

Es importante tener en cuenta que la gestión de TI debe procurar que TI no solo se centre en las actividades de soporte y mantenimiento de los sistemas existentes, de la misma forma TI debe centrarse en las necesidades reales de la organización; a su vez, debe converger a ser preactiva, buscar que los proyectos de TI se conviertan en operaciones o servicios (que a la larga es lo que dará valor a esos proyectos), igualmente buscará una mejora continua de los procesos así como la manera de justificar las inversiones.

Como se puede ver, hay diversas actividades que involucra la gestión de TI, John Thorpe (2005) propone unas disciplinas de Gestión de TI[2], de las cuales se hará una breve mención:

- **Planificación estratégica** que establece la dirección para el uso aceptable, eficaz y eficiente de la TI.
- **Arquitectura de empresa** para la planificación y el diseño global e interacción de los componentes dentro del negocio, incluyendo personas estructura y tecnología. Esta última incorpora infraestructura, software estructuras de datos.
- **Gestión del portafolio** para seleccionar la opción mejor de inversión.
- **Gestión de programas** para la supervisión global de los trabajos requeridos para entregar las inversiones acordadas.

[2] Disciplinas citadas de [CARR12].

- **Gestión de proyectos** para la planificación específica e implantación de una iniciativa aprobada.
- **Gestión de activos de TI** para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios.
- **Entrega de servicios operativos** que proporcionan una entrega sostenida eficaz, eficiente y aceptable de la capacidad operativa requerida de TI por la organización. Esta disciplina es conocida como **Gestión de los Servicios de TI.**
- **Seguridad de la Información** para la comprensión y el tratamiento del riesgo para disponibilidad, integridad, privacidad y autenticidad de la información que la organización crea y recoge durante el desarrollo del negocio.

Un marco de Gestión de TI agrupa la mayoría de actividades de la gestión requeridas es COBIT (*Control Objectives for Information and related Technology*), que es una guía de mejores prácticas enfocada a la Gestión de TI, que permite establecer un marco de referencia a través de los recursos que ofrece para su implementación, como un resumen ejecutivo, unos objetivos de control, mapas de auditoría, herramientas para implementación y una guía de técnicas de gestión. Es una iniciativa mantenida por ISACA (*Information Systems Audit and Control Association*) y el IT Governance Institute (*IT Governance Institute*).

2.4 Gestión de Servicios de TI

Las organizaciones se han visto obligadas a realizar una gestión adecuada de TI, y del mismo modo replantearse cómo entrega los servicios de TI a nivel interno y externo. Por esta razón, y de cara al beneficio del cliente, se planteó una forma de enfocar la entrega de servicios de TI basado en procesos y alineado con los objetivos de la organización, y se empieza a hablar de la Gestión de Servicios de TI GSTI (ITSM en inglés). La GSTI no solo aporta servicio de punta a punta sino también a la calidad del servicio, tiene en cuenta los diferentes aspectos que relacionan al negocio y a la tecnología, así como la conciencia que la cadena de provisión puede depender de proveedores externos o internos. De la misma manera como el servicio está alineado con los objetivos de negocio, logra que los procesos sean más eficientes y reduce los riesgos asociados a los servicios.

La GSTI establece una base de conocimiento que le permite monitorizar los procesos de provisión del servicio y realizar su seguimiento bajo ciertos parámetros definidos.

Actualmente las organizaciones implementan ciertos marcos para la GSTI que le permiten seguir códigos de mejores prácticas, como es el caso de la Librería de Infraestructura de TI ITIL (en inglés *Information Technology Infrastructure Library*).

Figura 3. Visión General de ITIL[3]

A pesar que ITIL propone un marco de mejores prácticas, es un estándar de facto, no es certificable. Para demostrar que se implementa un sistema de gestión de servicios de TI (SGSTI) se utiliza como referencia la norma internacional para gestión de servicios de TI ISO/IEC 20000. La certificación para esta norma permite demostrar de una forma independiente a los clientes que la entidad cumple con las mejores prácticas en gestión de servicios de TI, y es totalmente compatible con ITIL.

[3]OSIASTIS. ITIL Fundamentos de la Gestión TI. ¿Qué es ITIL? [http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php]

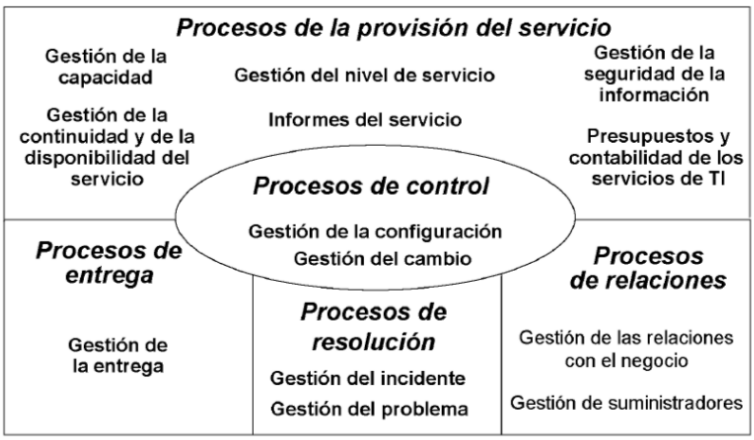

Figura 4. Procesos de la Gestión de Servicio [ISO20000]

2.5 Gobernanza y Gestión de la Seguridad de la Información

La Información como activo importante de las organizaciones, tiene un mayor protagonismo dentro de la Gobernanza de TI, la Gestión de TI y la Gestión de Servicios de TI.

Se propone un concepto de Gobernanza de la Seguridad de la información, que forme parte de la Gobernanza Corporativa y está alineada con la Gobernanza de TI, y que es responsabilidad del consejo de administración y dirección ejecutiva, la parte del consejo requerirá que se integre a todos los procesos de negocio y que de este modo se pueda tener un control de los activos críticos de la organización, y la dirección ejecutiva se encargará de responder a cualquier preocupación y sensibilidad que surjan con relación a la seguridad de la información.[BENI12]

Como objetivo, la seguridad tendrá que garantizar la triada CIA (*Confidentiality*, *Integrity*, *Availability*) que se muestra en la Figura 5.

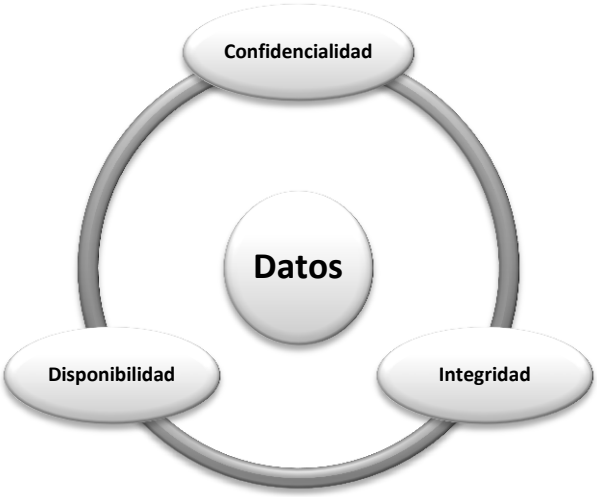

Figura 5. Triada CIA

De modo que se busca que se garantice que: la información se encuentra disponible y es utilizable cuando se requiere y cuando los sistemas que la proporcionan pueden resistir ataques de manera razonable y recuperarse de fallos (**disponibilidad**); La información es accedida por, o divulgada únicamente a aquellas personas que tienen derecho a conocerla (**confidencialidad**); la información se encuentra protegida contra modificaciones no autorizadas (**integridad**). Adicionalmente, que las transacciones de negocio, así como la información intercambiada entre ubicaciones de la empresa o entre socios comerciales puede ser confiada (**autenticidad y no repudio**). [BENI12].

Actualmente no hay alguna norma que soporte la gobernanza de la seguridad de la información, pero si hay códigos de mejores prácticas para establecer una buena estrategia de seguridad que respalde la gobernanza de la seguridad de la información y que realiza la gestión de la seguridad de la información.

Una norma que es certificable en las organizaciones es la ISO 27001, que establece los requisitos necesarios para implementar un Sistema de Gestión de la Seguridad de la Información SGSI (en inglés *Information Security Management Systems* ISMS).

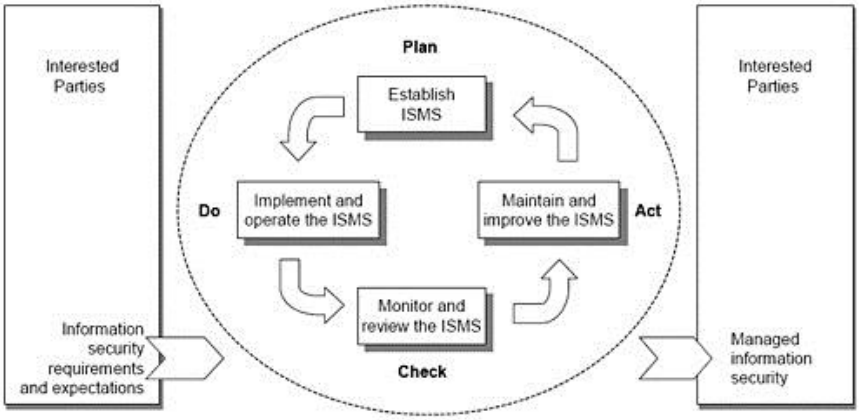

Figura 6. Modelo PDCA aplicado a SGSI [ISO27001]

2.6 Gestión de la Continuidad del negocio

Para la organización, no sólo es necesario asegurar sus activos de información, sino también que sus sistemas de información estén disponibles cuando se necesiten. La organización debe preocuparse por mantener sus funciones con un nivel mínimo aceptable durante una contingencia, bien sea un desastre natural, corte en suministro, fallo en sistemas, sabotajes, etc., todo esto con el fin que mantenga su estrategia y la consecución de los objetivos de la organización. Por esta razón las organizaciones desarrollan e implementan lo que se conoce como Plan de Continuidad del Negocio BCP (en inglés *Business Continuity Plan*).

La ventaja de considerar un marco para la continuidad del negocio, es que ayuda a las organizaciones a sobreponerse a amenazas que puedan interferir su operación normal. El BCP debe contemplar todas las medidas preventivas y de recuperación para cuando se produzca una contingencia que afecte al negocio. Con el BCP, la organización proyecta su actuación en futuros incidentes que puedan poner en peligro los intereses y la consecución de la misión de la organización.

A nivel de estándar, existe la BS 25999-2 (*Business continuity management. Specification*) que se trata de una norma certificable en la que se tiene como objeto la Gestión o Plan de la Continuidad del Negocio fundamentalmente enfocado a la disponibilidad de la información. Cuenta también con un código de mejores prácticas.

Hace algunos meses se lanzó una norma internacional y es la norma ISO 22301:2012 Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio – Requisitos.

Estas dos normas son bastante similares, pero la ISO 22301 puede ser considerada como una actualización de la BS 25999-2. Esta norma recopila conocimiento de especialistas y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización.

ISO 22301 establece un marco formal de continuidad del negocio y proporciona los lineamientos para desarrollar un plan de continuidad del negocio.

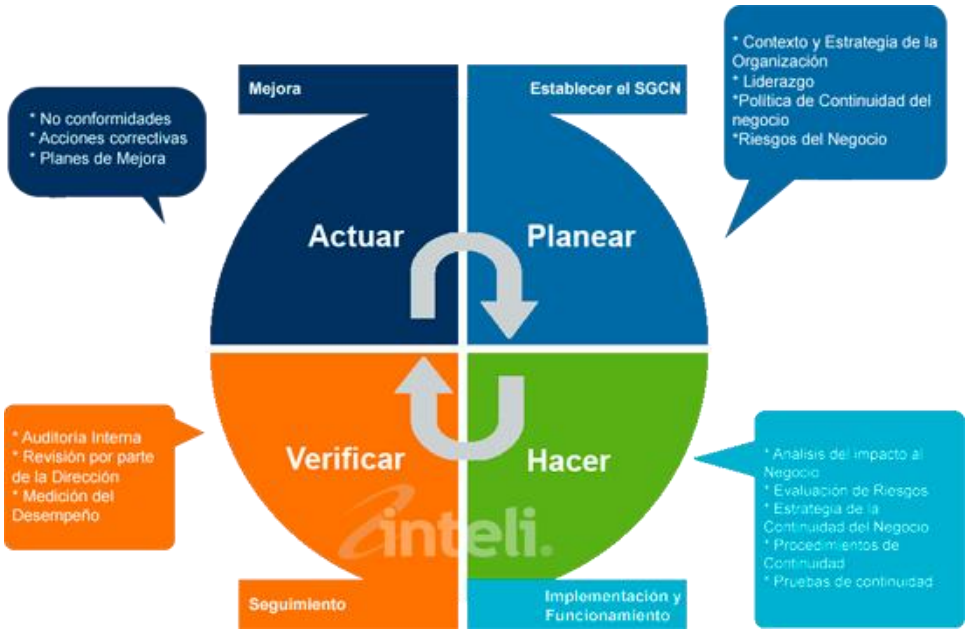

Figura 7. Ciclo PDCA para la Gestión de la Continuidad del Negocio[4]

2.7Gestión del Riesgo

Un concepto común para las áreas de conocimiento ya vistas es el Riesgo. Antes de definir el Riesgo en general, es necesario tener claros los conceptos de amenaza y vulnerabilidad, pues serán útiles para el concepto de riesgo y para el desarrollo del tema de estudio. Una amenaza puede definirse como la probabilidad de ocurrencia de un evento de cierta magnitud que puede comprometer un activo (tangible o intangible) en la organización, y la vulnerabilidad es la debilidad de uno o un grupo de activos que puede ser explotada por una o varias amenazas. En función de estos dos conceptos se puede decir que el Riesgo es la probabilidad de que una amenaza se materialice aprovechando vulnerabilidades existentes en un activo o un grupo de activos.

[4]Alfonso Tercero. 2012. *La Norma ISO 22301 para la Gestión de la Continuidad del Negocio*. Inteli. [http://www.inteli.com.mx/portal/images/stories/ciclo_pdca_inteli.png]

También se define el riesgo en una ecuación básica como la suma de una condición y una consecuencia. La condición viene asociada a las amenazas, que son ejecutadas por un actor y un motivo y que a través de una vulnerabilidad genera un resultado –la explotación de esa vulnerabilidad, exposición o debilidad puede ser voluntaria o involuntaria–; a la condición se le asocia con la probabilidad de ocurrencia. La consecuencia se refiere a los efectos sobre uno de los activos como resultado de la explotación realizada, y esto se asocia al impacto en la organización. [CEBU11].

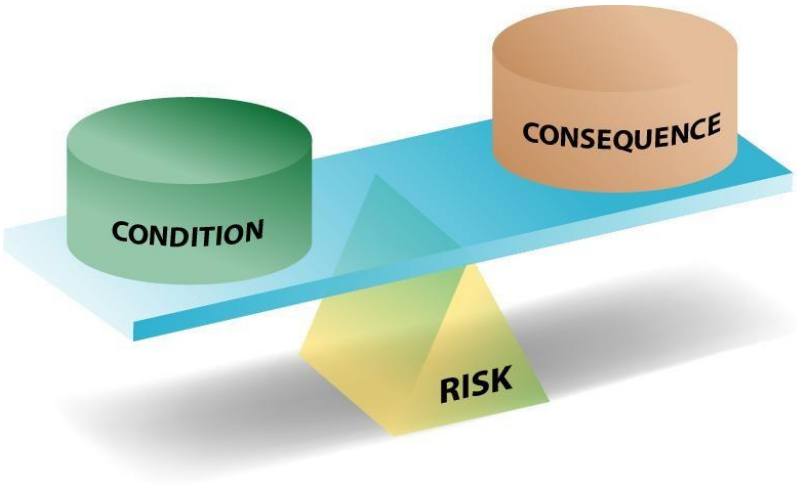

Figura 8. La ecuación básica del Riesgo. [CEBU11]

Hay varios tipos de Riesgo Empresarial, que hace una visión holística de todas las actividades de riesgos en la organización y considera todos los tipos de riesgos. En lo que concierne a este trabajo, nos centraremos en el Riesgo Operacional, que es uno de los cuatro tipos de riesgo generalmente aceptados junto a Riesgo de Peligros (Naturales), Financieros y Estratégicos. A pesar de esto, se pueden presentar riesgos superpuestos entre los diferentes tipos –un riesgo de peligro (Inundación o Incendio) puede afectar un riesgo operacional o un riesgo estratégico puede incluir riesgos financieros–. [CEBU11]. Para efectos de entendimiento definiremos el riesgo operacional como un riesgo que afecta la operación normal del negocio o que puede interferir en el alcance de los objetivos del negocio o la consecución de la misión.

Dentro de las organizaciones es claro que debe establecerse un marco para la gestión de riesgos, esto con el fin de mantener a salvo sus activos frente a amenazas, fortalecer sus vulnerabilidades y tratar el riesgo (bien sea controlándolo, aceptándolo, evitándolo o transfiriéndolo). Esto se hace a través de la Gestión de Riesgo Empresarial ERM (en inglés

Enterprise Risk Management), que establece metodologías que en general realizan una planeación de la metodología y establecimiento del contexto del riesgo, caracterización e identificación del Riesgo, Análisis de Riesgo, Evaluación de riesgo, Tratamiento de Riesgo y esto en un ambiente continuo de monitorización y revisión y de comunicación y consulta. Con respecto al Riesgo Operacional, la gestión se hace a través de un subconjunto de ERM y es la Gestión de Riesgo Operacional ORM (*Operational Risk Management*).

2.8 Resiliencia operacional

Antes de llegar al análisis de lo que es Resiliencia operacional, primero se debe definir el concepto de Resiliencia. Hay diferentes definiciones en diversos campos, sin embargo tomaremos la definición de WordNet: "Propiedad física de un material cuando puede volver a su posición o forma original después de una deformación que no excede su límite elástico"[5].

La definición de resiliencia considerada anteriormente, fue adaptada por el CERT (*Computer Emergency Response Team*) del SEI (*Software Engineering Institute*) de Carnegie Mellon, quienes definen la Resiliencia operacional "Resiliencia operacional es la propiedad **emergente** de una **organización** que puede **continuar llevando a cabo su misión** después de una **interrupción** que no excede su límite **operacional**"[6] [CRMM10].

Es un hecho que las organizaciones cada vez tienen mayor complejidad, y se desarrollan en ambientes complejos tanto a nivel de negocio como operativo. Dicha complejidad ha hecho que se enfrenten a situaciones de estrés e incertidumbre que provocan interrupciones en la operación efectiva de la organización. Este estrés puede ser producido por la masificación de los avances tecnológicos y la tecno-dependencia de la compañía para hacer eficaces los procesos de negocio y por tanto la complejidad que añade la tecnología a nivel de vulnerabilidades y riesgos; también lo produce la evolución de las organizaciones a nivel de proveedores, asociaciones, *outsourcing*, etc., crean nuevos ambientes de riesgo; así como la globalización y expansión geográfica de las organizaciones que les obliga a considerar nuevos riesgos y amenazas. [CRMM10]

[5] Traducido por Autor. Original: *"The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit"* [wordnet.princeton.edu].
[6] Traducido por Autor. Original: *"Operational Resilience is the emergent property of an organization that can continue to carry out its mission after disruption that does not exceed its operational limit"* [CRMM10].

La importancia de considerar la resiliencia operacional en las organizaciones, como se puede ver, es su aportación a la Gobernanza Corporativa, pues será una medida para garantizar que se consiga la misión de la organización, manteniendo operativos los servicios en condiciones degradadas, y este sería el fin de establecer un marco de Gestión de Resiliencia operacional.

A diferencia de los temas indicados anteriormente, no hay estándares definidos, pero si se encontró un modelo realizado por el CERT del SEI, y es el Modelo de Gestión de Resiliencia (CERT *Resilience Management Model*) CERT-RMM, que es definido como "una manera innovadora y transformadora de abordar el reto de gestionar la resiliencia operacional en ambientes complejos y con riesgos en evolución. Es el resultado de años de investigación sobre las formas en que las organizaciones gestionan la seguridad y la supervivencia de los activos que aseguran el éxito de la misión. Incorpora conceptos de una comunidad en procesos de mejora establecidos que permite a las organizaciones madurar holísticamente sus capacidades de seguridad, continuidad del negocio, y gestión de operaciones de TI y mejorar la previsibilidad y éxito en las operaciones de sostenimiento cuando se produce una interrupción." [CRMM10][7]

La gestión de la resiliencia operacional deberá considerar la complejidad de estos ambientes, y como base se tendrá que considerar los riesgos que implican cada actividad. En el modelo CERT-RMM consideran el concepto de "convergencia" como fundamental para la gestión de la resiliencia operacional. Se define convergencia como la armonización de las actividades de gestión de riesgo operacional que tienen objetivos y resultados similares. Dentro de las actividades considera:

1. Planeación y Gestión de la Seguridad,
2. Gestión de la Continuidad del Negocio y Recuperación de desastres, y la
3. Gestión de Operaciones y Entrega de Servicios de TI y
4. Gestión de servicios de TI.

[7] Traducido por Autor. Original: "*is an innovative and transformative way to approach the challenge of managing operational resilience in complex, risk-evolving environments. It is the result of years of research into the ways that organizations manage the security and survivability of the assets that ensure mission success. It incorporates concepts from an established process improvement community to allow organizations to holistically mature their security, business continuity, and IT operations management capabilities and improve predictability and success in sustaining operations whenever disruption occurs*" [CRMM10]

Otras actividades de apoyo pueden involucrarse, como la gestión financiera, las comunicaciones, gestión de recursos humanos y capacitación organizacional y sensibilización. Ver Figura 9. [CRMM10].

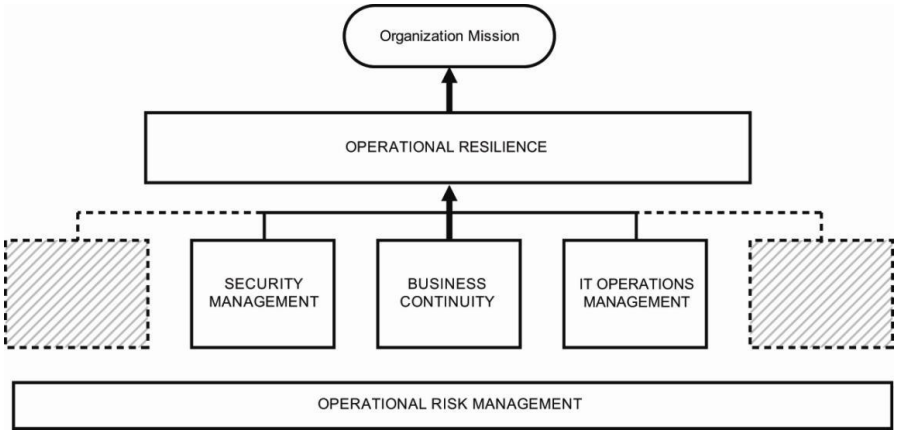

Figura 9. Convergencia de las Actividades de la Gestión de Riesgo Operacional [CRMM10]

CERT-RMM indica que las organizaciones han llegado a entender que estas tres áreas involucran funciones con la misma meta, mejorar y sostener la resiliencia operacional. La importancia de la convergencia es que cuando funciones y actividades llegan a compartir los mismos objetivos, soluciones y competencias, se puede realizar un alcance común. También se pueden eliminar actividades redundantes (y costos asociados), se puede establecer colaboración entre actividades que tienen objetivos similares y que se hace un enfoque hacia la misión. La convergencia afecta directamente el nivel de resiliencia operacional y afecta la habilidad para cumplir la misión de la organización.

Esta convergencia de conceptos de Gestión de TI, Gestión de servicios de TI, Seguridad de la Información y Continuidad del Negocio con la Resiliencia operacional nos da idea de lo que quiere lograr a modo general para las organizaciones, y es establecer un soporte a los riesgos comunes y alinear las prácticas de cada área con el fin de obtener el mayor beneficio para el alcance de la misión de la organización ofreciendo los servicios no solo con las mejores prácticas sino en cualquier situación, de manera óptima en funcionamiento normal, y de manera productiva en condiciones de estrés o interrupción a través de la Gestión de la Resiliencia operacional.

El modelo CERT-RMM está influenciado por diferentes bases de conocimiento y modelos, además de códigos de mejores prácticas, marcos y estándares mencionados anteriormente como ISO 27001, COBIT, ITIL, BS25999 y CMMI[8](Figura 10).

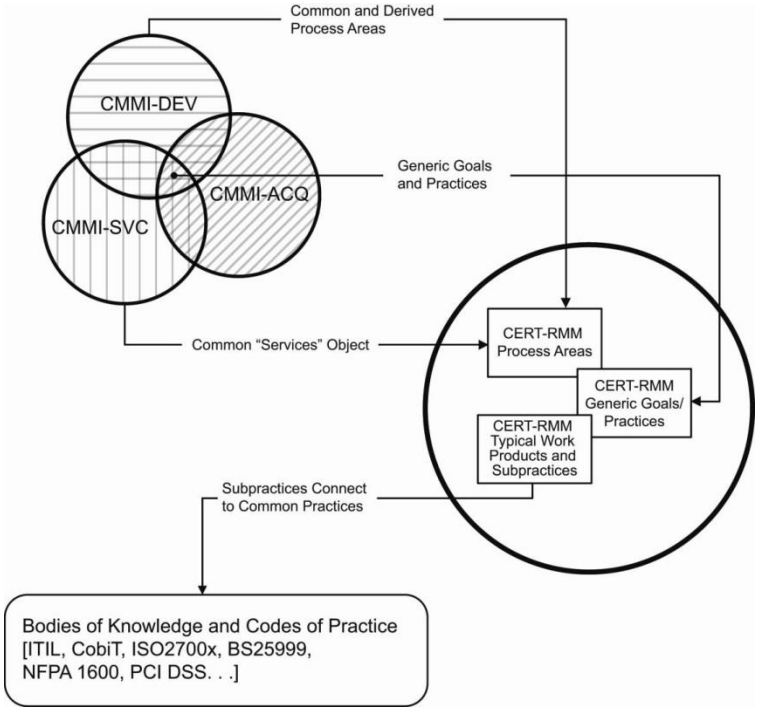

Figura 10. Influencias de CERT-RMM [CRMM10]

"La resiliencia operacional dirige la capacidad de la organización para adaptarse a los riesgos que afectan sus capacidades operacionales básicas. Es una propiedad emergente de la gestión de riesgos operacional eficaz y eficiente". [CRMM10].

La Gestión de la Resiliencia operacional se encargará de la definición de procesos y prácticas relacionadas que una organización utiliza para diseñar, desarrollar, implementar y controlar las estrategias para proteger y mantener (por ejemplo, hacer operacionalmente resiliente) los

[8] "Integración de modelos de madurez de capacidades o *Capability maturity model integration* (CMMI) es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software.
Las mejores prácticas CMMI se publican en los documentos llamados modelos. En la actualidad hay tres áreas de interés cubiertas por los modelos de CMMI: Desarrollo, Adquisición y Servicios.

La versión actual de CMMI es la versión 1.3 la cual corresponde a CMMI-SVC, liberada el 1 de noviembre de 2010. Hay tres constelaciones de la versión 1.2 disponible:

- CMMI para el Desarrollo (CMMI-DEV o CMMI for Development), Versión 1.2 fue liberado en agosto de 2006. En él se tratan procesos de desarrollo de productos y servicios.
- CMMI para la adquisición (CMMI-ACQ o CMMI for Acquisition), Versión 1.2 fue liberado en noviembre de 2007. En él se tratan la gestión de la cadena de suministro, adquisición y contratación externa en los procesos del gobierno y la industria.
- CMMI para servicios (CMMI-SVC o CMMI for Services), está diseñado para cubrir todas las actividades que requieren gestionar, establecer y entregar Servicios."

[http://es.wikipedia.org/wiki/Capability_Maturity_Model_Integration]

servicios de alto valor (organizacionalmente críticos), los procesos de negocio relacionados y activos asociados como personas, la información, tecnología, y activos. En resumen, la gestión de la resiliencia operacional tiene cuatro objetivos:

1. Prevenir la ejecución de un riesgo operacional en un servicio de alto valor (instancia de estrategia de protección),
2. Mantener el servicio de alto valor si la amenaza del riesgo se lleva a cabo (instancia de estrategia de sostenibilidad),
3. Tratar de manera efectiva las consecuencias que tiene en la organización que el riesgo se ejecute,
4. Devolver a la organización a un estado de operación "normal" y por último optimizar el logro de estos objetivos para maximizar la eficacia al menor costo. [CRMM10].

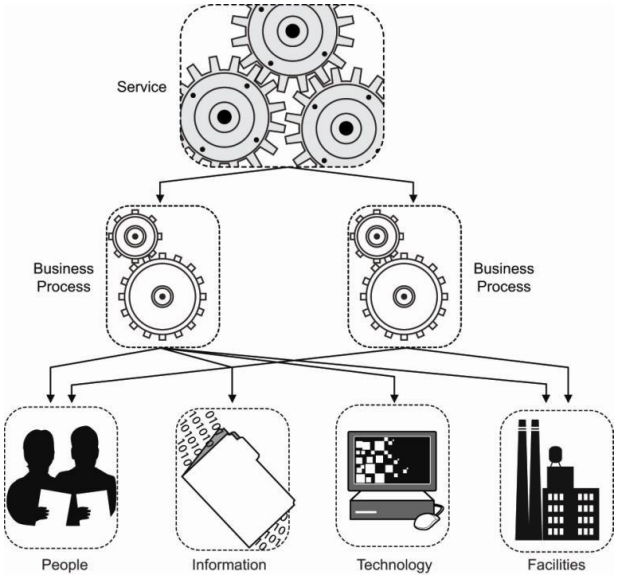

Figura 11. Relación entre Servicios, Procesos de Negocio y Activos [CRMM10]

La resiliencia dependerá de la relación entre servicios, procesos de negocio y activos (Ver Figura 11), y son elementos a considerar a la hora de gestionar la resiliencia operacional:

- ***Servicios:*** Los servicios los define CERT-RMM como un número limitado de actividades que la organización ejecuta para entregar un servicio o para producir un producto. Se hará en especial énfasis en los servicios de alto valor, los cuales son críticos para el alcance de la misión de la organización. por lo tanto se espera que por ser los que directamente apoyan el logro de objetivos estratégicos, estén protegidos y

sostenidos para minimizar interrupciones. La misión del servicio debe habilitar la misión de la organización.

- ***Procesos de Negocio:*** Son actividades o tareas que la organización que contribuyen a la consecución de la misión del servicio y son transversales a la organización. Un Servicio está soportado por uno o más procesos del negocio. La misión de un proceso debe habilitar la misión del servicio

- ***Activos:*** Es algo de valor para la organización. Se definen cuatro tipos de activos, Personas, Información, Tecnología e Instalaciones que en están estrechamente relacionados en contexto (Ver Figura 12).

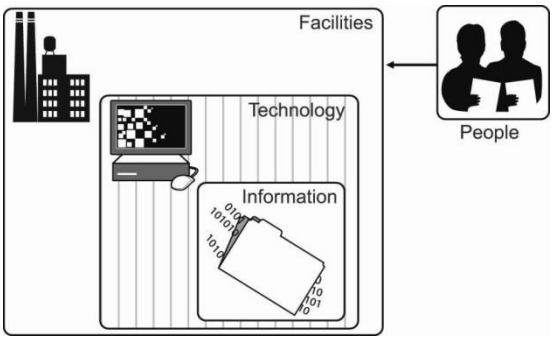

Figura 12. Tipos de activos puestos en contexto [CRMM10]

Los activos de alto valor tienen Propietarios y Vigilantes. Los Propietarios son personas o unidades organizaciones, internas o externas a la organización que tienen una responsabilidad primaria por la viabilidad, productividad y resiliencia del activo. Los Vigilantes son personas o unidades organizaciones, internas o externas a la organización que están de acuerdo y son responsables de implementar y gestionar los controles para satisfacer los requisitos de resiliencia de los activos de alto valor mientras están bajo su cuidado. En todos los casos, los propietarios son los responsables de asegurar la protección y continuidad apropiada de sus activos, sin tener en cuenta las acciones (o inacciones) de los vigilantes. [CRMM10].

Los servicios y procesos de negocio se componen de activos, el impacto de la interrupción de un activo afecta a uno o más procesos de negocio, este puede afectar la misión de un servicio y por lo tanto la misión de la organización (Figura 13).

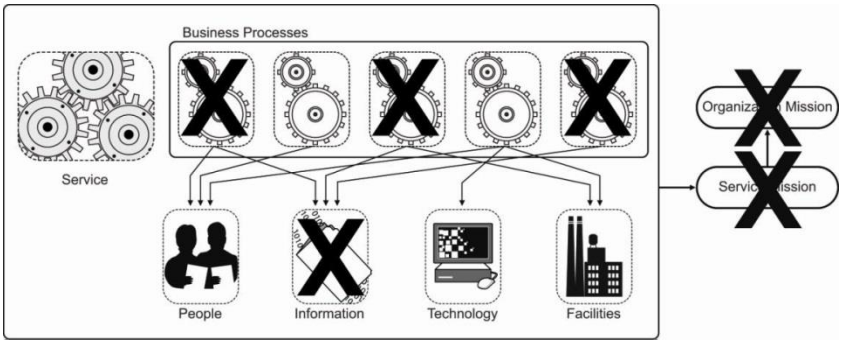

Figura 13. Impacto de la interrupción de un activo en la misión de un servicio [CRMM10]

Por lo tanto, a nivel de activos empieza la definición de resiliencia operacional, pues protegiendo a los activos de amenazas y riesgos puede garantizar la capacidad de recuperación operativa del servicio, además los activos deben ser sostenibles –capaces de ser recuperados y restaurados a cierto estado o condición de operación– durante tiempos de interrupción y estrés. Por lo tanto se deben gestionar las condiciones de riesgo, que es la parte de protección, y gestionar las consecuencias del riesgo, que es la parte de sostenibilidad (Ver Figura 14). Para esto se definen estrategias de protección a través de actividades destinadas a minimizar la exposición de los activos a amenazas, interrupciones y explotación de vulnerabilidades, se definen a través de procesos, procedimientos, políticas y controles; y estrategias de sostenimiento a través de actividades destinadas a mantener los activos en su normalidad en cuanto sea posible en situaciones de estrés o interrupción, se definen a través de procesos, procedimientos, políticas y controles.

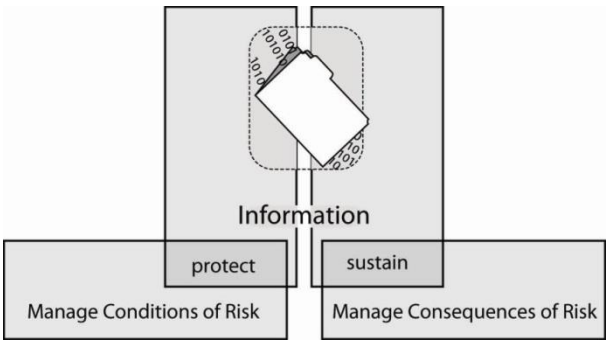

Figura 14. Optimización de Resiliencia de Activo de Información [CRMM10]

Como se evidencia, la gestión de la resiliencia operacional estará ligada a los servicios a través de la protección y sostenimiento de los activos, y ayudará a mantener el alcance de la misión del servicio –y por tanto la misión de la organización– en situaciones de estrés o interrupción a través de la relación que se muestra en la Figura 15.

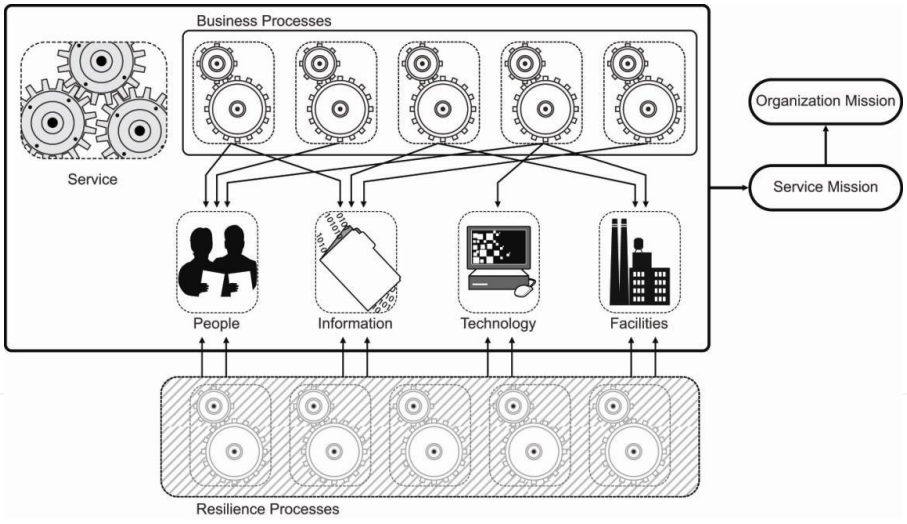

Figura 15. Relación entre Servicios y Procesos de Gestión de Resiliencia operacional [CRMM10]

Como se mencionó anteriormente, CERT-RMM utiliza también CMMI como base de conocimiento y con base a él define áreas de proceso y prácticas/metas genéricas. CERT-RMM tiene 26 áreas de proceso (PA) que están organizadas dentro de cuatro categorías de resiliencia operacional de alto nivel: Ingeniería, Gestión Empresarial, Operaciones y Gestión de Procesos (Ver Tabla 1). Por área de proceso hay 3 metas genéricas y 13 prácticas genéricas, además de 94 metas específicas y 251 prácticas específicas.

Categoría	Etiqueta	Área de Proceso
Ingeniería	ADM	Definición y Gestión de Activos
Ingeniería	CTRL	Gestión de Controles
Ingeniería	RRD	Desarrollo de Requisitos de Resiliencia
Ingeniería	RRM	Gestión de Requisitos de Resiliencia
Ingeniería	RTSE	Ingeniería de Soluciones Técnicas Resilientes
Ingeniería	SC	Continuidad del Servicio
Gestión Empresarial	COMM	Comunicaciones
Gestión Empresarial	COMP	Cumplimiento
Gestión Empresarial	EF	Enfoque Empresarial
Gestión Empresarial	FRM	Gestión de Recursos Financieros
Gestión Empresarial	HRM	Gestión de Recursos Humanos
Gestión Empresarial	OTA	Formación y Conciencia Organizacional
Gestión Empresarial	RISK	Gestión de Riesgos
Operaciones	AM	Gestión de Acceso
Operaciones	EC	Control del Entorno
Operaciones	EXD	Gestión de Dependencias Externas
Operaciones	ID	Gestión de Identidades
Operaciones	IMC	Gestión y Control de Incidentes
Operaciones	KIM	Gestión de Información y Conocimiento
Operaciones	PM	Gestión de Personas
Operaciones	TM	Gestión de la Tecnología
Operaciones	VAR	Análisis y Resolución de Vulnerabilidades
Gestión de Procesos	MA	Medición y Análisis
Gestión de Procesos	MON	Monitorización
Gestión de Procesos	OPD	Definición de Proceso Organizacional
Gestión de Procesos	OPF	Enfoque de Proceso Organizacional

Tabla 1. Áreas de proceso por categoría y etiqueta asociada [CRMM10]

2.9 Resiliencia Software

La Tecnología de la Información y la comunicación, son parte fundamental en las organizaciones, no solo para las que prestan servicios basados en TI, sino para todas las que utilizan Sistemas de Información. El Software y los Sistemas son activos ubicuos en las organizaciones que automatizan servicios y soportan procesos de negocio, que ayudan a la organización a la consecución de la misión. Para organizaciones dónde es vital el uso de software y sistemas en cualquier circunstancia y en las cuales se debe mantener el servicio así sea en condiciones degradadas, es necesario considerar la resiliencia como una opción.

Teniendo una idea general sobre Resiliencia operacional, haremos énfasis en lo que concierne a la Resiliencia Software. Teniendo en cuenta la definición de Resiliencia operacional en el CERT-RMM, se puede decir que la Resiliencia Software es la habilidad de un software para recuperarse y ajustarse a sí mismo en situaciones de interrupción o estrés logrando ejecutar la tarea para la cuál ha sido diseñado, apoyando los servicios de la organización.

Para hacer software resiliente que sobreviva y sea resistente a amenazas es necesario establecer un compromiso organizacional que dirija la resiliencia a través del proceso de desarrollo. Esto quiere decir, que el software debe estar diseñado y desarrollado considerando las amenazas a las que se va a enfrentar, las condiciones de funcionamiento y el ambiente cambiante de riesgos en los cuales va a operar, así como las prioridades y necesidades de sostenimiento de los servicios que soportan. [CRMM10].

Para una organización que enmarcada en la Gobernanza de TI tenga una gestión de la resiliencia organizacional sobre sus activos de software, debe cerciorarse que de acuerdo a sus necesidades, no sólo el software desarrolle sus requisitos funcionales, sino que se realice bajo unos parámetros de calidad y cumpliendo unos parámetros de seguridad, disponibilidad, rendimiento, confiabilidad y sostenibilidad.

No todas las organizaciones están expuestas a las mismas amenazas, ni deben garantizar resiliencia en los mismos servicios, para cada organización la planeación de la resiliencia software es distinta, los requisitos de resiliencia de la organización son diferentes. Siguiendo el esquema de relaciones propuesto en CERT-RMM y que se mostró en la **Figura 15,** la gestión de la resiliencia se hará sobre el activo software, pero se deberán considerar ciertos aspectos:

- Las organizaciones deben tener claros los requisitos a nivel de seguridad, disponibilidad, rendimiento, confiabilidad y sostenibilidad del software.

- Las organizaciones deben ser conscientes que a nivel de negocio y operaciones, el software puede ser construido, adquirido o contratado como servicio, por lo que debe tener una visión global del software, ya a su vez tener en cuenta conceptos como ciclo de vida y madurez.

- Las organizaciones deben tener un entendimiento del entorno complejo de riesgos al que se enfrentan, por lo tanto deberán considerar los escenarios para los cuáles se desea estar preparado, cuáles tienen mayor impacto para la consecución de la misión o se consideran críticos, cuáles tienen mayores vulnerabilidades a estrés o interrupción, y frente a qué amenazas la organización hará al software resiliente.

- Las organizaciones deben establecer responsabilidades sobre dichos activos, establecer propietarios y vigilantes.

- Es casi imposible que un software sea resiliente en todos los escenarios, pero de ser esto un requerimiento es importante complementar la resiliencia con planes de contingencia y continuidad.

Utilizar software resiliente en las organizaciones, tiene sus ventajas y también desventajas que tendrán que ser consideradas de acuerdo a los intereses de la organización.

Ventajas	Desventajas
• Ideal para organizaciones que requieren que sus sistemas trabajen por largos periodos de tiempo. • Blindar la operación frente a "fuerzas externas". • Reducir pérdidas a la organización, pues garantiza la misión del servicio y por ende la de la organización. • Visión del activo software en función de Protección y Sostenibilidad.	• Aumenta la complejidad al sistema. • Puede incrementar el tiempo de desarrollo y mantenimiento. • Mayor coste de desarrollo • Mayor formación de las personas que lo han de desarrollar • No está al alcance de todas las organizaciones.

Tabla 2. Ventajas y Desventajas del Software Resiliente

2.10 Calidad de Software

Las organizaciones comprometidas con la calidad de sus procesos, servicios y productos, buscan la manera de garantizar que cada área sigue unas estrategias de acuerdo a unas mejores prácticas que les facilite el entendimiento y la aplicación de la calidad tanto en los procesos, servicios y productos.

A nivel de software esto no es una excepción. Las empresas buscan que su software (*in-house* o externo), cumpla con ciertos parámetros de calidad, pero entonces en ¿qué consiste la calidad del software? Hay que tener claro que la calidad de software puede referirse a la parte funcional, es decir, el cumplimiento de cierto modelo basado en los requisitos

funcionales o especificaciones. Y a la parte estructural, que son requisitos no funcionales que apoyan la entrega de los requisitos funcionales[9].

La calidad del software no es certificable, se certifican los procedimientos para construir software de calidad, para esto se consideran modelos de madurez y guías de mejores prácticas. Y aunque la calidad no es certificable, si hay estándares internacionales para evaluar la calidad del software como el modelo de calidad ISO 25000:2005.

Sin embargo, La resiliencia del software no es una característica que actualmente se evalúe dentro de estas normas, pero si hay iniciativas para garantizar de cierto modo un grado de seguridad en el software que contribuyen a la resiliencia de software.

2.11 Aseguramiento del Software (Software Assurance SwA)

Software Assurance (SwA) es definido como "el nivel de confianza de que un software está libre de vulnerabilidades, tanto si son diseñadas intencionadamente dentro del software o accidentalmente introducidas en cualquier momento durante su ciclo de vida, y que el software funciona de manera prevista"[10]. De este modo busca asegurar que los procesos, procedimientos y productos usados para producir y sostener el software, sean conformes a todos los requisitos establecidos, y de la misma manera esto puede hacer los sistemas software mucho más seguros.

Aunque es un concepto que surge a nivel gubernamental (*US Government*), es aplicable a empresas que deseen garantizar calidad y seguridad en el software. Su objetivo es tener una visión global del ciclo de vida del software que incluya las personas, procesos y tecnología que permita garantizar la protección del software crítico con el fin de mantener la misión de la organización.

En [GHAN11] encontramos un interesante esquema de áreas de conocimiento y esfuerzos claves que se debe tener en cuenta a la hora de considerar SwA y que se ve en la Figura 16. Destacamos que considera tanto los Procesos y Prácticas (*Processes and Practices*), donde se considera mejoras al Ciclo de Vida del desarrollo, Modelos de Madurez de Capacidad, Modelos de Madurez y prácticas para mitigar debilidades en el software y la parte de

[9] [http://en.wikipedia.org/wiki/Software_quality].
[10] Traducido por Autor. Original: "the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner." [http://en.wikipedia.org/wiki/Software_assurance]

Adquisición y externalización *(Acquisition and Outsourcing),* que considera aspectos de la adquisición, compra, contratos, además de gestión de riesgo. Estos aspectos podrán ser guía a la hora de plantear la influencia de la resiliencia software tanto para el construido *in-house*, como el adquirido o contratado. Hay otros aspectos que podrían ser considerados luego a través del desarrollo de la guía.

Figura 16. Áreas de Conocimiento y Esfuerzos en SwA [GHAN11]

3. EVALUACIÓN DE RIESGOS

Debido al enfoque de este estudio, más que la evaluación de riesgos de un proyecto de resiliencia en una organización, nos centraremos en la evaluación de riesgos que se debe establecer a la hora de pensar en la implantación de un proyecto de resiliencia operacional, y específicamente de resiliencia del software, esto último debido a que la resiliencia de software sería una implementación organizacional que tiene la intención de reducir el impacto de una amenaza que produce una interrupción o estrés del servicio.

La organización debe establecer una buena práctica para la organización de la gestión de riesgos, como se mencionó anteriormente, hay algunos marcos establecidos para gestionar los riesgos de una organización (ERM) tales como la ISO 31000, y los cuáles serán el marco general del riesgo operacional y específicamente el riesgo operativo del software que produce interrupciones en los procesos de negocio, por ende a la misión del servicio y finalmente a la misión de la organización.

El software, así como otro tipo de activos, debe considerarse como una inversión. Diversas metodologías de gestión de proyectos de TI establecen un análisis financiero para la cartera de proyectos de TI de la organización, esto implica que se hagan estimaciones de tiempos y costes (p. ej. de desarrollo, de pruebas, de implantación…), y que se calcule la Tasa Interna de Retorno (TIR) que lo hará más atractivo a la hora de invertir, sin olvidar, que las estimaciones son valoraciones que pueden variar significativamente al momento en que el proyecto se materializa. Debido a los riesgos que trae consigo la inversión en proyectos software, es necesario establecer un marco de riesgos sobre el proceso, y no sobre el producto –como se suele hacer–, debido a que esta visión (construcción, adquisición o contrato de software), nos permitirá considerar el alcance que se ajusta a los intereses del negocio.

Considerando que el software puede ser adquirido, desarrollado o contratado como servicio, se debe tener un cuidado específico en cada caso, debido a que de las prácticas que se establezcan en el desarrollo dependerá el éxito de la solución a nivel de requisitos de resiliencia, y en el caso de un Software como Servicio SaaS, el proveedor debe brindar todas las garantías dentro del SLA (*Service Level Agreement*), y en el caso de adquisición se debe hacer un estudio de si la

solución adquirida cumplirá con los requisitos de disponibilidad e integridad que requiere la organización.

Es necesario que la organización identifique, analice y mitigue los riesgos enmarcado en las definiciones de tolerancia y apetencia que defina la organización, todo esto con el fin que se mantenga a salvo sus activos frente a amenazas y logre la consecución de los objetivos de la organización. A nivel de riesgo operacional, entendiendo el riesgo asociado a servicios y activos vinculados a la operación habitual de la organización, puede ser el resultado de un potencial impacto debido a un fallo de los procesos internos, una acción inadvertida o deliberada de una persona, problemas con sistemas o tecnología y eventos externos. [CRMM10]

El objeto de este estudio no es establecer diferentes marcos de riesgos que se relacionen con el desarrollo, adquisición o contrato de software, sin embargo sí es importante mencionar que la gestión de riesgos en cada uno de los casos no es la misma. De hecho, encontramos marcos para la gestión de riesgos de software que considera los diversos casos como el de la Figura 17.

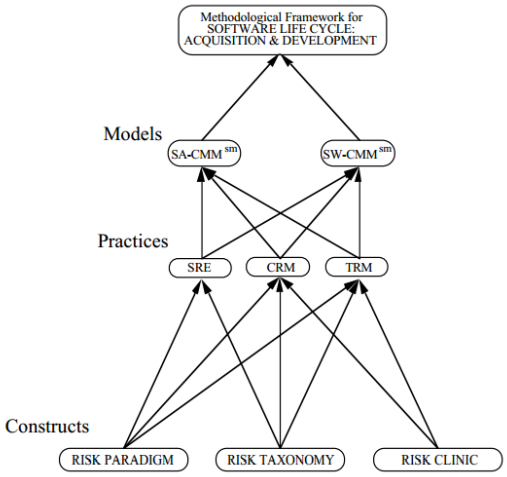

Figura 17 Marco metodológico para la gestión de riesgos de software[11]

La organización que considere implantar la resiliencia de software debe tener un marco de gestión de riesgos que considere las diferentes opciones de acuerdo a su operación:

- Construcción de Software: Dentro del marco de gestión de riesgos se debe establecer los riesgos relacionados con el diseño, implementación de una solución y específicamente los riesgos relacionados con la operación de los servicios de la organización. Preguntas

[11] Higuera, R-. Haimes, Y. (1996). *Software Risk Management*. Software Engineering Institute. Carnegie Mellon University.

comunes: ¿Qué riesgos pueden presentarse durante el desarrollo que afecten la operación normal de un servicio? ¿A qué amenazas se verá enfrentado el software que soporta el servicio? ¿Qué etapas del ciclo de vida son más vulnerables y debo ser más estricto con la gestión de riesgos?

- Adquisición de Software: El marco de gestión de riesgos debe considerar los riesgos relacionados a la ingeniería de adquisición y procesos relacionados que afecten la operación de los servicios en la organización. Preguntas comunes: ¿La solución está diseñada para funcionar en condiciones degradadas en caso de estrés o interrupción? ¿Qué riesgos está dispuesto a asumir la organización con el software que piensa adquirir?

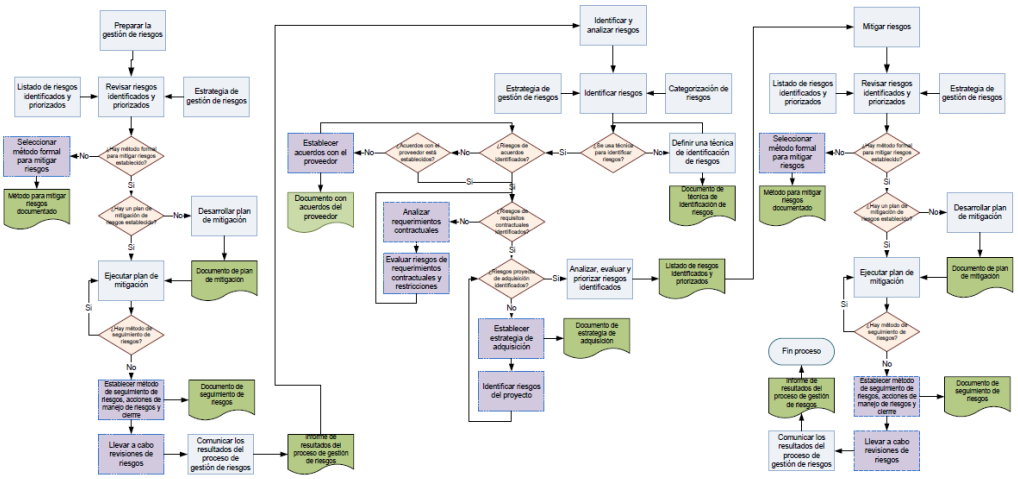

Figura 18. Ejemplo de Marco de gestión de riesgos para adquisición de software[12]

- Contrato de Software: Con la oportunidad que han tenido las organizaciones de contratar Software como servicio gracias al *Cloud Computing*, se han generado nuevos ambientes de riesgos que deben ser considerados en las organizaciones, sobre todo aquellos servicios software que estén relacionados con objetivos de la organización. Preguntas comunes: ¿El acuerdo del nivel de servicio considera riesgos relacionados con peligros naturales? ¿El proveedor de servicios brinda una gestión de riesgos que garantiza los requerimientos de la organización a nivel de disponibilidad e integridad?

[12] Gasca Hurtado, G. (2010). *Metodología de gestión de riesgos para la adquisición de software en pequeños entornos - MEGRIAD*. Tesis Doctoral. Facultad de Informática. Universidad Politécnica de Madrid.

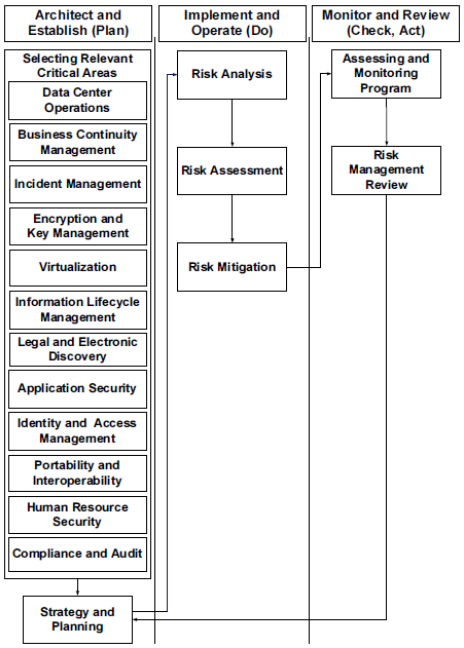

Figura 19. Ejemplo de Marco de gestión de riesgos para entornos basados en Cloud Computing[13]

Conscientes de que hay un marco de riesgos que enmarca las amenazas que se pueden presentar en cada uno de los tipos de activos de la organización –en nuestro caso software–, a nivel operacional el CERT en su modelo de resiliencia propone un área de proceso que considera Gestión de Riesgos RISK como apoyo a la resiliencia operacional. El propósito de esta área es identificar, analizar y mitigar los riesgos a los activos de la organización que pueden afectar de manera negativa la operación y entrega de servicios.

El área de proceso RISK establece la responsabilidad de la organización para desarrollar e implementar un plan y un programa para ORM, con base en el ERM, que cubra de manera comprensiva y cooperativa los servicios y activos de alto valor de la organización. A su vez esto estará alineado con la tolerancia y apetito de riesgos que estén definidos en la estrategia de la organización. En la Tabla 3 se encuentran las metas y prácticas asociadas al área de proceso RISK.

Metas	Prácticas
RISK:SG1 Preparación para la Gestión de Riesgos	RISK:SG1.SP1 Determinar las categorías y fuentes de Riesgo
	RISK:SG1.SP2 Establecer una estrategia para la Gestión de Riesgo Operacional

[13] Zhang, X. Wuwong, N. Li, H. Zhang, X. (2010). *Information Security Risk Management Framework for the Cloud Computing Environments*. 10th IEEE International Conference on Computer and Information Technology.

RISK:SG2 Establecer parámetros y enfoque de Riesgos	RISK:SG2.SP1 Definir los parámetros de Riesgo
	RISK:SG2.SP2 Establecer criterios de medida del Riesgo
RISK:SG3 Identificar el Riesgo	RISK:SG3.SP1 Identificar los Niveles de riesgo en los Activos
	RISK:SG3.SP2 Identificar los Niveles de riesgo en los Servicios
RISK:SG4 Analizar el Riesgo	RISK:SG4.SP1 Evaluar Riesgos
	RISK:SG4.SP2 Categorizar y Priorizar Riesgos
	RISK:SG4.SP3 Asignar disposición al Riesgo
RISK:SG5 Mitigar y controlar el Riesgo	RISK:SG5.SP1 Desarrollar planes para la mitigación del riesgo
	RISK:SG5.SP2 Implementar estrategias de Riesgo
RISK:SG6 Usar la información de Riesgo para gestionar la resiliencia	RISK:SG6.SP1 Revisar y ajustar estrategias para proteger los activos y servicios
	RISK:SG6.SP2 Revisar y ajustar estrategias para sostener los servicios

Tabla 3. Metas y Prácticas del área de proceso Gestión de Riesgos RISK [CRMM10]

Una crítica a la gestión de riesgos en las organizaciones es la teoría del cisne negro o *Black Swan*, propuesta por Nassim Taleb: "Lo que aquí llamamos un Cisne Negro (y con mayúscula) es un evento con los tres atributos siguientes. En primer lugar, es un caso atípico, ya que se encuentra fuera del ámbito de las expectativas regulares, porque no hay nada en el pasado que puede apuntar de manera convincente a su posibilidad. En segundo lugar, conlleva a un impacto extremo. En tercer lugar, a pesar de su condición de rareza, la naturaleza humana nos hace inventar explicaciones de su presencia después de los hechos, por lo que es explicable y predecible.

Me detengo y resumo el triplete: rareza, impacto extremo y retrospectiva (aunque no prospectiva) previsibilidad. Una pequeña cantidad de Cisnes Negros explica casi todo en nuestro mundo, desde el éxito de las ideas y las religiones, a la dinámica de los acontecimientos históricos, hasta los elementos de nuestra vida personal."[14]

Y es entonces cuando se piensa si realmente es suficiente la gestión de riesgos establecida, o si realmente la organización está preparada para los diferentes riesgos, si prefiere los de bajo impacto y alta frecuencia o los de alto impacto y baja frecuencia, y esto será determinante a la hora de considerar el factor de resiliencia operacional que debe ser implantado. En ocasiones se le da mayor importancia a los riesgos que se presentan con alta frecuencia y bajo costo, sin embargo esto puede representar un gasto de recursos en eventos triviales que no representan una alta amenaza para la operación.

De la misma manera las organizaciones deben pensar que esas amenazas que consideran improbables y a los cuales apenas da importancia, pueden ser su *Black Swan*. Por tanto tiene que

[14] Traducido por Autor, original [http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html?_r=0]

estar preparada y considerar escenarios en los cuales las situaciones se pueden materializar, y que operativamente le puede representar un impacto alto, y que debe preparar medidas que le ayuden a proteger y sostener los activos. Es claro que las organizaciones tienden a tener estructuras más complejas, depender mucho más de las relaciones, e inclusive considerar que su ubicación es un factor decisivo a la hora de estimar ciertos riesgos –por ejemplo la situación interna de un país puede ser una amenaza ya sea por conflicto o terrorismo, pero al mismo tiempo la ubicación de un proveedor de Cloud puede incurrir en incumplimiento a nivel legal–.

Según PriceWaterhouseCoopers en el artículo "*Black swans turn grey, The transformation of risk*"[15] las juntas directivas se fijan en tres cambios en los ambientes de control de riesgos, el primero es que sienten que los marcos y proceso de riesgos que siguen actualmente en la organización no les da el nivel de producción que necesitan. El segundo es que ven que incrementa tanto la velocidad en la que los eventos de riesgo toman lugar, como la extensión en la cual su impacto en el negocio es "contagioso", lo que quiere decir que se extiende por las diferentes categorías de riesgo, con una preocupación mayor sobre la velocidad y contagio de los riesgos catastróficos, que pueden amenazar la existencia de la organización e inclusive la industria entera. El tercer cambio es que se siente que se gasta mucho tiempo y dinero en los actuales procesos de gestión de riesgos, en vez de considerar los ambientes cambiantes para actuar de manera rápida y flexible en la identificación y ataque de nuevos riesgos, e inclusive algunas directivas consideran que no se justifica el gasto en el ERM frente al retorno de nivel de protección.

Por esto PriceWaterhouseCoopers propone tres pasos para ir más allá del ERM:

1. Desarrollar una cultura de conciencia de riesgos.
2. Un enfoque explícito sobre el apetito de riesgos y
3. Un alineamiento entre riesgo y estrategia.

La resiliencia operacional hace parte del primer paso, pues va más allá de identificar, medir y priorizar los riesgos, e intenta proteger y sostener los activos que le da mayor valor a la organización debido al servicio que prestan y adicionalmente desarrolla la cultura de conciencia de riesgos en la organización.

[15] [http://www.pwc.com/im/en/publications/assets/Black_swans_turn_grey.pdf]

En cierto modo, lo que se puede analizar es que el marco de gestión de riesgos es útil pero no suficiente, y que considerando un modelo de resiliencia obtenemos un mayor ajuste a la incertidumbre que generan las organizaciones hoy en día, no solo por su constitución y su dependencia, sino también por la cantidad de riesgos cambiantes y los *Black Swan*, que pueden afectar los servicios e impactar de manera negativa a la organización. La gestión de riesgos en la organización y específicamente los riesgos relacionados con el software que soporta los servicios de la organización, deben ser considerados con una visión holística la cual permita en lo posible establecer medidas para su protección y sostenimiento considerando todo el ciclo de vida.

Basado en este breve análisis, es preciso pensar que la resiliencia operacional será uno de los retos para las organizaciones, y que debido la dependencia que tienen en el software y los sistemas gran parte de los servicios de las organizaciones, es preciso establecer unas prácticas que le permitan cumplir parte de la resiliencia operacional a través de la resiliencia de software.

4. DESARROLLO

La necesidad de la Resiliencia en el Software se origina por la Resiliencia de los Servicios que ofrece la organización, tanto a nivel de negocio como a nivel de operación. Vamos a tomar el modelo CERT-RMM como base para el desarrollo de la guía, pero adicionalmente definiremos unos tipos de software para el negocio, pues para cada uno se deberá plantar una guía ajustada y unas recomendaciones que pueden diferir.

4.1 Tipos de Software

Hay varias tipologías de software, por funcionalidad, por área de conocimiento, por prácticas implementadas, por sectores de la industria, etc. Sin embargo la visión que se considerará en este estudio, es tipo de software por la responsabilidad que tiene la organización sobre él y por el proceso que requiere, es decir, si la compañía hace el software, contrata a un tercero para su construcción, lo adquiere a una tercera parte, o lo contrata como un servicio. De este modo tenemos cuatro tipos de software:

- **Software construido *in-house*:** La organización tiene un área de desarrollo encargada de construir y mantener el software a nivel interno.
- **Software construido por externos:** La organización contrata a un externo para desarrollar una aplicación a medida. (*Outsourced Development*)
- **Software adquirido:** Es cuando la compañía adquiere un software a una tercera parte (*Packaged Software*)
- **Software como servicio contratado:** Con la importancia actual de las aplicaciones en *Cloud*, es necesario considerar cuando la compañía contrata el acceso a un servicio que se ajusta a sus requisitos, que corresponde a un software que ya está desarrollado. A diferencia del software empaquetado, las responsabilidades cambiarán de manera drástica, por lo tanto se dejó diferenciado del anterior tipo.

Sin embargo, aunque tenemos estos tipos, tenemos un denominador común para cualquier tipo de software o sistema, ya sea desarrollando, adquiriendo o contratando la solución, todas requieren un proceso específico, y ahí es donde se tendrá en cuenta la resiliencia, sobre el proceso que requiere el activo software, para ser desarrollado o adquirido.

4.2 Áreas de Proceso CERT-RMM y Tipos de Software

Como se indicó anteriormente, se utilizará el CERT-RMM y realizaremos una visión a las áreas de proceso que proponen, con especial énfasis en las que aporten a la guía para la resiliencia software en las organizaciones. El CERT-RMM en la figura 20 se indica qué relaciones hay en ciertas áreas de proceso que corresponden a la gestión de resiliencia operacional de la tecnología. Lo que se realizó fue resaltar aquellas relaciones que implicaban el interés para la guía, es decir las relacionadas con construcción/adquisición/contrato de servicio de software. Encontramos interesante que el área de proceso Gestión de la Tecnología relaciona la mayoría de estos procesos, y por tanto podemos utilizar un marco de gestión de T.I. como referencia para desarrollar las implicaciones de la resiliencia en el software para la organización y poder establecer la guía, que es el resultado de este trabajo.

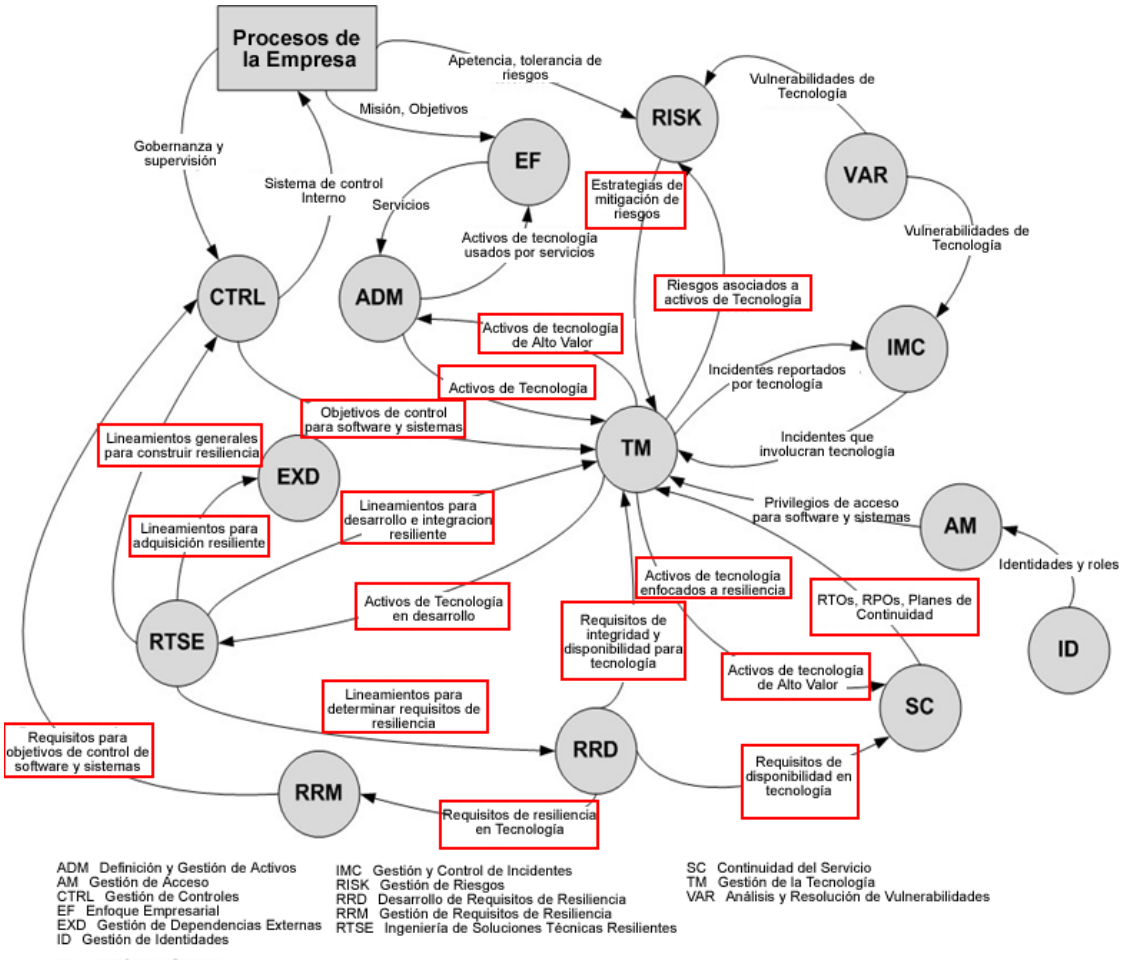

Figura 20. Relaciones que abordan la resiliencia de tecnología [CRMM10] resaltado por Autor

Revisando el CERT-RMM, encontramos que la mayoría de las áreas de proceso implicadas pertenecen a la categoría de *Ingeniería.* Los procesos que están incluidos en la categoría de *Ingeniería*, corresponden a los que se enfocan en establecer e implementar la resiliencia para los activos, procesos de negocio y servicios de la organización, a través de procesos guiados por requisitos. De este modo, establecen la base de la resiliencia y lo básico para proteger y sostener los activos, por ende los procesos de negocio y los servicios, como se explicó anteriormente.

Dentro de esta categoría hay tres subcategorías,

1. una correspondiente a la Gestión de Requisitos –Aborda el desarrollo y gestión de los objetivos de seguridad (proteger) y resiliencia (sostener) de los activos y servicios– (En esta subcategoría se encuentran las áreas de proceso *Desarrollo de Requisitos de Resiliencia* RRD y *Gestión de Requisitos de Resiliencia* RRM),

2. Gestión de Activos –Establece los activos más importantes para la organización– (En esta subcategoría se encuentran el área de proceso *Definición y Gestión de Activos* ADM) y

3. Establecimiento y gestión de la resiliencia – Aborda la gestión de controles preventivos, el desarrollo e implementación de la continuidad del servicio y gestión de impacto, y consideración del ciclo de vida de los atributos de calidad de la resiliencia para software y sistemas– (En esta subcategoría se encuentran las áreas de proceso *Gestión de Controles* CTRL, *Ingeniería de Soluciones Técnicas Resilientes* RTSE y *Continuidad del Servicio* SC). [CRMM10].

Los procesos incluidos en *Ingeniería* pueden realizar un aporte significativo a la definición de la guía, esto debido a que podremos tomar los objetivos que implican el desarrollo de soluciones resilientes para la organización, sin embargo esto sería solo una parte de lo que implica la resiliencia de software para la aplicación, teniendo en cuenta que el software no solo se desarrolla, adquiere, sino que también puede contratarse como servicio. Para la guía se debe considerar también el vacío que existe en la continuidad del negocio a nivel software, por esta razón tenemos un aporte importante con la sección de continuidad del servicio. Se deberá considerar conceptos de esquema de exigencia y cierres estructurados.

Volvamos a la Figura 20. Hay un área de proceso adicional que no se ha tenido en cuenta y que se encuentra en las relaciones que se han subrayado de la resiliencia operacional de tecnología, y es la EXD *Gestión de Dependencias Externas*. Esta pertenece a la categoría *Operaciones*, y a la subcategoría Gestión de Proveedores, la cual aborda la gestión de dependencias externas y su impacto en la resiliencia operacional de la organización. En esta parte podemos aplicar metas que definan lineamientos para los contratos en el software como servicio.

Para efectos de la guía desarrollaremos estas áreas de proceso consideradas en el CERT-RMM.

- *Definición y Gestión de Activos* ADM.
- *Desarrollo de Requisitos de Resiliencia* RRD.
- *Gestión de Requisitos de Resiliencia* RRM.
- *Gestión de Controles* CTRL.
- *Ingeniería de Soluciones Técnicas Resilientes* RTSE.
- *Continuidad del Servicio* SC.
- *Gestión de Dependencias Externas* EXD.
- *Gestión de la Tecnología* TM

4.2.1 Definición y Gestión de Activos ADM

Algo principal en la organización es considerar al software un activo más, un elemento que soporta un proceso de negocio, por lo tanto apoya un servicio y en consecuencia el logro de la misión de la organización. Pero es necesario tenerlo identificado, saber cuál es realmente crítico, establecer responsabilidades sobre la resiliencia del software en la organización, y tener un punto de partida.

En CERT-RMM, el propósito de esta área de proceso de definición y gestión de activos es identificar, documentar y gestionar activos de la organización durante su ciclo de vida para garantizar la productividad sostenida de los servicios de apoyo de la organización. [CRMM10].

Es claro que en una organización que se establece un marco de gobernanza de TI, y que sigue un marco de referencia de TI debe contar con este aspecto, lo cual

facilitaría el cumplimiento y la organización de la resiliencia operacional. Las metas específicas de esta área de proceso es establecer los activos, establecer relaciones entre activos y servicios y gestionar los activos.

Haciendo énfasis en la resiliencia software, para poder llevar a cabo estas metas específicas, es necesario que la organización cuente con un proceso que realice la gestión del software como activo, y con esto se plantearán actividades para identificar el software en la organización, establecer los propietarios y los vigilantes de cada software, asociar cada software al servicio que soporta, establecer los requisitos de resiliencia (para proteger y sostener) software acorde al servicio al que está asociado y de este modo valorar qué software es crítico (porque soporta un servicio de alto valor para la compañía) –esto lo aborda tanto las áreas de proceso *Desarrollo de Requisitos de Resiliencia* RRD y *Gestión de Requisitos de Resiliencia* RRM–. De la misma forma se debe relacionar con los procesos de gestión del cambio y estará alineado con la gestión del riesgo establecida para servicios de alto valor, y aportará al proceso de continuidad a través de *Continuidad del Servicio* SC.

Como se puede ver, este es el punto de partida a nivel de resiliencia operacional, y que se apoyará de la información que tenga la gestión de TI, recogerá la información de la mayoría de áreas de proceso y será el punto crítico para hacer la gestión de la resiliencia software. En la tabla 4 encontramos las Metas y Prácticas del Área de Proceso ADM.

Metas	**Prácticas**
ADM:SG1 Establecer Activos Organizacionales	ADM:SG1.SP1 Inventario de Activos
	ADM:SG1.SP2 Establecer un Entendimiento Común
	ADM:SG1.SP3 Establecer Propietarios y Vigilantes
ADM:SG2 Establecer relaciones entre Activos y Servicios	ADM:SG2.SP1 Asociar Activos con Servicios
	ADM:SG2.SP2 Analizar dependencias entre activos y servicios
ADM:SG3 Gestionar Activos	ADM:SG3.SP1 Identificar Criterios de Cambios
	ADM:SG3.SP2 Mantener Cambios a los Activos e Inventarios

Tabla 4. Metas y Prácticas del área de proceso Definición y Gestión de Activos ADM [CRMM10]

4.2.2 Desarrollo de Requisitos de Resiliencia RRD

Las organizaciones tienen prioridades sobre ciertos servicios, no todas funcionan igual, unas tienen mayor complejidad a nivel externo otras a nivel interno, a algunas

les preocupará la disponibilidad de ciertos servicios, a otras les interesa la continuidad, es decir, los requisitos de resiliencia varían de acuerdo a la misión de los servicios, por lo tanto a la misión de la organización. Como se dijo anteriormente, la criticidad de los servicios y los requisitos de resiliencia necesarios, dependerán de la evaluación que haga la organización sobre los servicios y por ende sobre los activos. En CERT-RMM, la identificación, documentación, análisis y gestión de los requisitos a nivel de los activos son abordados en las áreas de proceso *Desarrollo de Requisitos de Resiliencia* RRD y *Gestión de Requisitos de Resiliencia* RRM.

El propósito del área de proceso *Desarrollo de Requisitos de Resiliencia* RRD, es identificar, documentar y analizar los requisitos de resiliencia operacional para servicios de alto valor y sus activos relacionados. [CRMM10].

Si se realiza un análisis concienzudo sobre los requisitos de resiliencia en la práctica, estos se derivan de objetivos de la gestión de la seguridad (La triada CIA). Por lo tanto su definición dependerá del trabajo que realice la gestión de riesgos operaciones, teniendo en cuenta que los objetivos de la gestión de la seguridad se enfocarán a las amenazas a las que se exponen los activos, y por otra parte a lo que se defina en la continuidad del negocio. De este modo, estos requisitos serán inherentes al activo, como lo es su definición, valor y propietario.

Sobre estos requisitos se realizarán los procesos de ingeniería, por lo tanto se requiere que estén establecidos a nivel de empresa, servicio y activo.

El CERT-RMM sugiere que a nivel de resiliencia operacional de tecnología, los requisitos de resiliencia se centrarán en la integridad y disponibilidad.

Metas	**Prácticas**
RRD:SG1 Identificar requisitos empresariales	RRD:SG1.SP1 Establecer Requisitos de Resiliencia Empresarial
RRD:SG2 Desarrollar requisitos del servicio	RRD:SG2.SP1 Establecer Requisitos de Resiliencia de Activos
	RRD:SG2.SP2 Asignar Requisitos de Resiliencia Empresarial a los Servicios
RRD:SG3 Analizar y validar requisitos	RRD:SG3.SP1 Establecer una definición de la funcionalidad requerida
	RRD:SG3.SP2 Analizar Requisitos de Resiliencia
	RRD:SG3.SP3 Validar Requisitos de Resiliencia

Tabla 5. Metas y Prácticas del área de proceso Desarrollo de Requisitos de Resiliencia RRD [CRMM10]

Aplicado a nuestro objetivo, dependiendo de estos requisitos de resiliencia operacional a nivel de empresa y a nivel de servicio, se establecerán a nivel de software.

4.2.3 Gestión de Requisitos de Resiliencia RRM

Así como definir los requisitos de resiliencia tiene importancia para la organización, lo es de la misma forma la gestión de los requisitos durante su ciclo de vida. Los requisitos pueden cambiar en el tiempo si cambian los intereses de la organización, si se incorporan nuevos servicios, si hay nuevos riesgos e inclusive si se realiza algún cambio de tecnología. La organización tiene que monitorizar el rendimiento de sus requisitos y conforme lo necesite debe ajustarlos.

El propósito de esta área de proceso es gestionar los requisitos de resiliencia de los servicios de alto valor y activos asociados, e identificar inconsistencias entre esos requisitos y las actividades que la organización realiza para satisfacer los requisitos. [CRMM10].

De este modo, esta área de proceso asegura que los requisitos de resiliencia establecidos son efectivos y garantizan los objetivos en cuanto a protección y sostenimiento del activo y por ende del servicio. También se encarga de ajustarlos de acuerdo a los resultados que obtenga de la medición de la efectividad o de acuerdo a la dirección estratégica que establezca la organización.

El área de proceso *Gestión de Requisitos de Resiliencia* tiene un objetivo específico, y es gestionar los requisitos. Pero esto lleva unas prácticas para la organización, como el entendimiento de los requisitos, un compromiso de alcance y gestión de los requisitos, establecer trazabilidad, identificar inconsistencias, como se puede ver en la Tabla 6.

Metas	**Prácticas**
RRM:SG1 Gestionar Requisitos	RRM:SG1.SP1 Obtener un entendimiento de los Requisitos de Resiliencia
	RRM:SG1.SP2 Obtener un compromiso con los Requisitos de Resiliencia
	RRM:SG1.SP3 Gestionar los cambios en los Requisitos de Resiliencia
	RRM:SG1.SP4 Mantener la trazabilidad de los Requisitos de Resiliencia
	RRM:SG1.SP5 Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos

Tabla 6. Metas y Prácticas del área de proceso Gestión de Requisitos de Resiliencia RRM [CRMM10]

4.2.4 Gestión de Controles CTRL

Volvamos a la organización en general. El éxito de la organización dependerá del alcance de los objetivos que se plantearon a nivel organizacional, y que facilitan el alcance de la misión, y la manera de asegurar que esto se consigue es mediante la implantación eficaz y eficiente de los procesos de control interno incorporados al sistema de control interno de una organización. El sistema de control interno es la suma de las actividades que una organización emprende para garantizar el éxito en el alcance de su misión, objetivos y estrategias mediante los procesos de negocio definidos tal efecto.

El sistema de control interno se centra en la operación, pues se encarga de plantear políticas, procedimientos, métodos, tecnologías y herramientas que proporcionan la seguridad de que las directivas de gestión se llevan a cabo, pero también tiene otros objetivos con respecto a comportamiento ético, detección y prevención de fraude, garantizando cumplimiento e indicadores de desempeño. La política es un medio para la implementar las directrices de la dirección y minimizar el impacto de una amenaza en el éxito y logro organizacional. La manera como se refleja este cumplimiento, es el establecimiento de objetivos de control –como es el caso de COBIT a nivel IT– que deben estar alineados con lo que establezca la organización a nivel de requisitos –para la resiliencia, es evidente que esto será los requisitos de garantía de la misión del servicio y las estrategias para proteger y sostener los activos–

Desde la perspectiva de la gestión de la resiliencia operacional, estos controles operativos son fundamentales para la protección de los activos, el mantenimiento de los activos, y la prevención de las interrupciones de los activos a medida que se despliegan en la ejecución de un servicio. Dicho esto, la gestión efectiva de controles para la resiliencia operacional significa identificar las mejores estrategias de relación costo-efectividad para la protección y el mantenimiento de los bienes y servicios, establecer la combinación óptima. En esta área de proceso, la organización establece

objetivos de control que reflejan la misión y objetivos de la organización y define el objetivo para el desarrollo de controles a nivel empresa y operacional. [CRMM10]

El propósito de esta área de proceso es establecer, monitorizar, analizar y gestionar un sistema de control interno que asegure la eficacia y eficiencia de operaciones a través de asegurar el éxito de la misión de los servicios de alto valor y de los activos que los soportan. [CRMM10].

Teniendo en cuenta que el enfoque es el software, será necesario tomar los objetivos de control que estén relacionados con la adquisición, desarrollo o contrato del software, y el marco que se podría utilizar para este fin es COBIT, como se señaló anteriormente. Estos objetivos se alinearán al marco de gobernanza, y deberán garantizar que sigue el rumbo de la estrategia de la organización.

Las metas y prácticas asociadas del área de proceso *Gestión de Controles* se puede observar al detalle en la Tabla 7.

Metas	**Prácticas**
CTRL:SG1 Establecer Objetivos de Control	CTRL:SG1.SP1 Definir los objetivos de control
CTRL:SG2 Establecer Controles	CTRL:SG2.SP1 Definir los controles
CTRL:SG3 Analizar Controles	CTRL:SG3.SP1 Analizar los controles
CTRL:SG4 Evaluar efectividad de los Controles	CTRL:SG4.SP1 Evaluar los controles

Tabla 7. Metas y Prácticas del área de proceso Gestión de los Controles CTRL [CRMM10]

4.2.5 Ingeniería de Soluciones Técnicas Resilientes RTSE

Como se indicaba anteriormente, las organizaciones dependen mucho más de la automatización de servicios, y del mismo modo optan por utilizar el software para esos fines. Ya sea creando un área que soporte el desarrollo de aplicaciones o contratando a un tercero para el desarrollo de las mismas, el fin es el mismo, buscar que se resuelvan necesidades que surgen a la organización para prestar sus servicios internos o externos, pero también, dependiendo de los intereses de la organización, las soluciones que implementen tienen que tener en cuenta los requisitos de resiliencia establecidos, de modo que el servicio sea funcional en ocasiones de estrés o interrupción (Proteger y Sostener).

Teniendo establecidos los requisitos de resiliencia software y un marco de control, es preciso, al menos para los desarrollos *in-house* de aplicaciones, que la organización se asegure que existe un compromiso para que se desarrolle software que cumpla las necesidades de protección y sostenimiento para así alcanzar la misión del servicio y por tanto la de la organización, y para desarrollos contratados a externos, que de algún modo demuestren que las soluciones que construyen cumplen con los requisitos de resiliencia planteados. Para esto la organización debe entender cuáles son los servicios que desea mantener, a qué condiciones operacionales se enfrenta, qué situaciones de riesgo debe tener presente y qué amenazas puede afrontar.

La idea es que en el ciclo de vida del diseño y desarrollo de software no solo se contemple cumplimiento de los requisitos funcionales, sino que también contemple requisitos de calidad como seguridad, rendimiento, confiabilidad y sostenimiento.

Sin embargo, considerar estos requisitos en la organización implica un mayor esfuerzo y costo, y a la vez genera complejidad en los sistemas, por esto deben estudiar el beneficio que se va a obtener. Comúnmente estos requisitos no se tienen en cuenta o se dejan para lo último, y esto implica mayores riesgos en seguridad y en ocasiones es un costo mayor que podría haberse evitado implicando los requisitos de calidad desde el inicio, por eso tiene que evaluarse de la mejor manera de modo que la inversión que se haga en la resiliencia se justifique de la mejor manera.

El objetivo será que se garantice la integridad y disponibilidad del software a través de mejores prácticas para la implementación de medidas que se tendrán en cuenta desde el principio del ciclo de vida del desarrollo, para que el software tenga la capacidad de funcionar en condiciones degradadas en caso de interrupción o estrés –inclusive es importante contar con un plan de continuidad, pues no se puede hacer frente a todas las amenazas como se dijo anteriormente–

El propósito de esta área de proceso es asegurarse que el software y los sistemas están desarrollados para satisfacer los requisitos de resiliencia. [CRMM10].

Las metas y prácticas asociadas del área de proceso *Ingeniería de Soluciones Técnicas Resilientes* se puede observar al detalle en la Tabla 8.

Metas	Prácticas
RTSE:SG1 Establecer lineamientos para el desarrollo de soluciones técnicas resilientes	RTSE:SG1.SP1 Identificar las directrices generales
	RTSE:SG1.SP2 Identificar las directrices de Requisitos
	RTSE:SG1.SP3 Identificar las directrices de Arquitectura y Diseño
	RTSE:SG1.SP4 Identificar las directrices de Implementación
	RTSE:SG1.SP5 Identificar las directrices de Montaje e Integración
RTSE:SG2 Desarrollar planes para el desarrollo de soluciones técnicas resilientes	RTSE:SG2.SP1 Seleccionar y ajustar directrices
	RTSE:SG2.SP2 Integrar las directrices seleccionadas con un proceso definido de desarrollo de software y sistemas
RTSE:SG3 Ejecutar el Plan	RTSE:SG3.SP1 Monitorear la ejecución del plan de desarrollo
	RTSE:SG3.SP2 Entregar soluciones técnicas resilientes en producción

Tabla 8. Metas y Prácticas del área de proceso Ingeniería de Soluciones Técnicas Resilientes RTSE [CRMM10]

4.2.6 Continuidad del Servicio SC

Como se ha indicado, es muy difícil hacer que un activo sea resiliente a todas las condiciones. De la misma forma la organización puede establecer la mejor gestión de riesgos empresariales, y esto no la hace inmune a todas las amenazas o a un estado de "seguridad total". Por esta razón, las organizaciones deben estar preparadas para afrontar las consecuencias de interrupciones a nivel operativo que se le presentan, teniendo en cuenta que estas pueden suceder en cualquier momento, y que una interrupción significativa puede costarle demasiado. En el caso del activo software, las organizaciones deben entender que se tiene que contar con planes que puedan continuar la prestación de los servicios de TI cuando la interrupción del software es inminente.

La continuidad del servicio describe el proceso organizacional responsable del desarrollo, despliegue, ejercicio, implementación y gestión de planes de respuesta y recuperación de eventos y restauración de operaciones del negocio de modo habitual. [CRMM10]. La organización se debe comprometerse a establecer un plan y un programa para la continuidad del servicio, de igual manera darle los suficientes recursos e infraestructura, y gestionarlos y mantenerlos de forma adecuada.

Por otro lado, la continuidad del servicio deberá tener en cuenta la valoración de los servicios –pues la prioridad son los de alto valor–, los riesgos potenciales y las consecuencias para la organización.

El propósito de esta área de proceso es asegurar la continuidad de operaciones esenciales de servicios de servicios y activos relacionados, si una interrupción ocurre como resultado de un incidente, desastre u otro evento interruptor. [CRMM10].

Las metas y prácticas asociadas del área de proceso *Continuidad del Servicio* se puede observar al detalle en la Tabla 9.

Metas	Prácticas
SC:SG1 Preparar para la continuidad del servicio	SC:SG1.SP1 Planear la continuidad del servicio
	SC:SG1.SP2 Establecer estándares y directrices para la continuidad del servicio
SC:SG2 Identificar y priorizar servicios de alto valor	SC:SG2.SP1 Identificar los servicios de alto valor para la organización
	SC:SG2.SP2 Identificar dependencias e interdependencias internas y externas
	SC:SG2.SP3 Identificar los registros y bases de datos
SC:SG3 Desarrollar planes de continuidad del servicio	SC:SG3.SP1 Identificar los planes a ser desarrollados
	SC:SG3.SP2 Desarrollar y documentar los planes de continuidad del servicio
	SC:SG3.SP3 Asignar personal a los planes de continuidad del servicio
	SC:SG3.SP4 Almacenar y asegurar los planes de continuidad del servicio
	SC:SG3.SP5 Desarrollar el plan de formación para la continuidad del servicio
SC:SG4 Validar planes de continuidad del servicio	SC:SG4.SP1 Validar los planes con requisitos y estándares
	SC:SG4.SP2 Identificar y resolver los conflictos del plan
SC:SG5 Ejercer planes de continuidad del servicio	SC:SG5.SP1 Desarrollar programas y normas de pruebas
	SC:SG5.SP2 Desarrollar y documentar planes de prueba
	SC:SG5.SP3 Ejercer planes
	SC:SG5.SP4 Evaluar los resultados de las pruebas sobre el plan
SC:SG6 Ejecutar planes de continuidad del servicio	SC:SG6.SP1 Ejecutar planes
	SC:SG6.SP2 Medir la Efectividad del plan en operación
SC:SG7 Mantener planes de continuidad del servicio	SC:SG7.SP1 Establecer criterios de cambio
	SC:SG7.SP2 Mantener los cambios a los planes

Tabla 9. Metas y Prácticas del área de proceso Continuidad del Servicio SC [CRMM10]

4.2.7 Gestión de Dependencias Externas EXD

Con el auge del *outsourcing*, las empresas con límites abiertos, e inclusive con las dependencias de proveedores y clientes, la organización debe considerar la importancia de las entidades externas dentro de la resiliencia operacional de la organización. La organización da acceso a estas entidades externas a activos, y por esto debe considerar los posibles riesgos que esto implica y tomar las medidas

necesarias para la protección de los activos y garantizar que con esto se ejecute la misión de los servicios.

Para el caso del software, cuándo una tercera empresa es subcontratada para el desarrollo está claro que va a tener un acceso significativo a los sistemas de la organización, del mismo modo si se contrata a una tercera parte, debemos asegurar que esta establece unos mecanismos adecuados de gestión para la prestación de los servicios.

Según [CRMM10] en el caso de soportar un servicio, una entidad puede:

- Usar sus propios activos. Si una entidad externa falla para en la protección y sostenimiento de estos activos, el servicio y sus resultados pueden verse comprometidos –si la organización por ejemplo contrata software como servicio SaaS, el *Acuerdo de Nivel de Servicio* SLA será clave en la manera como presta el servicio y por tanto cómo actúa en casos de estrés o interrupción–.

- Acceder a los activos de la organización (el cual incluye la habilidad de controlar o modificar los activos). Las acciones de la entidad externa pueden afectar la resiliencia de los activos y de este modo comprometer el servicio – en el caso de Software construido por externos, se deben tomar medidas para el acceso que tendrá el equipo de desarrollo contratado a los recursos de la organización y en especial al activo que se puede comprometer–

- Poseer y usar los activos de la organización (lo que incluye la responsabilidad del cuidado de esos activos). Si la entidad externa no cumple los requisitos de resiliencia de los activos, (especificados por la organización), hay un impacto potencial en la misión del servicio – en el caso de Software construido por externos, debe establecerse por las partes un compromiso para el buen uso de los activos y para seguir los lineamientos definidos sobre resiliencia organizacional, enfocándose en la misión de servicio que dependa de software.

- Desarrollar, entregar, encargar o instalar un activo nuevo o revisado para la organización.

- Proveer servicios de soporte que ayuden en la protección y sostenimiento de un activo de la organización.

El propósito de esta área de proceso es establecer y gestionar el nivel de controles para asegurar la resiliencia de los servicios y activos que dependen de las acciones de entidades externas. [CRMM10].

Las metas y prácticas asociadas del área de proceso *Gestión de Dependencias Externas* se puede observar al detalle en la Tabla 10.

Metas	Prácticas
EXD:SG1Identificar y priorizar dependencias externas	EXD:SG1.SP1 Identificar dependencias externas
	EXD:SG1.SP2 Priorizar dependencias externas
EXD:SG2 Gestionar los riesgos debido a dependencias externas	EXD:SG2.SP1 Identificar y evaluar riesgos debido a dependencias externas
	EXD:SG2.SP2 Mitigar riesgos debido a dependencias externas
EXD:SG3 Establecer relaciones formales	EXD:SG3.SP1 Establecer especificaciones empresariales para dependencias externas
	EXD:SG3.SP2 Establecer especificaciones de resiliencia para dependencias externas
	EXD:SG3.SP3 Evaluar y seleccionar entidades externas
	EXD:SG3.SP4 Formalizar relaciones
EXD:SG4 Gestionar desempeño de entidades externas	EXD:SG4.SP1 Monitorear rendimiento de entidades externas
	EXD:SG4.SP2 Corregir rendimiento de entidades externas

Tabla 10. Metas y Prácticas del área de proceso Gestión de dependencias externas EXD [CRMM10]

4.2.8 Gestión de la Tecnología TM

Como se ha dicho anteriormente, los activos de tecnología son de gran importancia en las organizaciones, y mucho más por el apoyo a los procesos de negocio, que logran la consecución de la misión de los servicios y por ende de la organización. Desde esta perspectiva, la tecnología inmersa en las operaciones de la organización, hace un aporte significativo a nivel competitivo y estratégico.

En el caso del software, es un activo de tecnología de importancia porque será fundamental para soportar un servicio –o servicios– específicos, por lo que se debe

establecer una gestión en cuanto a requisitos de resiliencia y relación con servicios refiere.

Como se ha indicado en secciones anteriores, la gestión de TI se encargará de dirigir la función de TI, y en cuanto a resiliencia operacional orientará la importancia del activo de tecnología frente a un servicio específico de modo que se tenga como directiva la integridad y disponibilidad del mismo. Sin embargo, es en esta área de proceso donde se indicará claramente las prioridades y el enfoque de la resiliencia sobre la tecnología, por lo tanto sobre el software que es el objeto de este estudio. Aquí se relacionarán todas las áreas de proceso y se soportará al marco de gestión de TI que se establezca.

El propósito de esta área de proceso es establecer y gestionar un nivel apropiado de controles relacionados a la integridad y disponibilidad de los activos de tecnología para soportar las operaciones resilientes de servicios organizacionales. [CRMM10].

Las metas y prácticas asociadas del área de proceso *Gestión de la Tecnología* se puede observar al detalle en la Tabla 11.

Metas	**Prácticas**
TM:SG1 Establecer y priorizar activos de tecnología	TM:SG1.SP1 Priorizar los activos de tecnología
	TM:SG1.SP2 Establecer los activos tecnológicos enfocados en la Resiliencia
TM:SG2 Proteger los activos tecnológicos	TM:SG2.SP1 Asignar Requisitos de Resiliencia a los Activos de Tecnología
	TM:SG2.SP2 Establecer e Implementar Controles
TM:SG3 Gestionar riesgo de los activos de tecnología	TM:SG3.SP1 Identificar y evaluar los riesgos de activos de tecnología
	TM:SG3.SP2 Mitigar los Riesgos Tecnológicos
TM:SG4 Gestionar la integridad de los activos de tecnología	TM:SG4.SP1 Controlar el acceso a los activos de tecnología
	TM:SG4.SP2 Ejecutar la gestión de la configuración
	TM:SG4.SP3 Ejecutar la gestión y control del cambio
	TM:SG4.SP4 Ejecutar la gestión de la entrega
TM:SG5 Gestionar la disponibilidad de los activos de tecnología	TM:SG5.SP1 Ejecutar la planeación para el sostenimiento de activos de tecnología
	TM:SG5.SP2 Gestionar el mantenimiento de los activos de tecnología
	TM:SG5.SP3 Gestionar la capacidad de la tecnología
	TM:SG5.SP4 Gestionar la interoperabilidad de la tecnología

Tabla 11. Metas y Prácticas del área de proceso Gestión de la Tecnología TM [CRMM10]

Además de las áreas planteadas, es necesario que en cada área de proceso se considere las prácticas genéricas que define el CERT-RMM para cada área de proceso (Ver Tabla 12) –

Correspondiente al compromiso, gestión e implantación de las prácticas en la organización alineado con el negocio–, que es junto con el proceso de *Gestión de Riesgos* es fundamental en las consideraciones de resiliencia de software pues será la base y proporcionará las entradas de las amenazas a las cuales hacer frente.

Metas	Prácticas
GG1 Lograr metas específicas	GG1.GP1 Desarrollar prácticas específicas
GG2 Institucionalizar un proceso gestionado	GG2.GP1 Establecer una gobernanza del proceso
	GG2.GP2 Planear el proceso
	GG2.GP3 Proveer recursos
	GG2.GP4 Asignar responsabilidades
	GG2.GP5 Entrenar al personal
	GG2.GP6 Gestionar las configuraciones del producto de trabajo
	GG2.GP7 Identificar e involucrar a los stakeholders relevantes
	GG2.GP8 Monitorear y controlar el proceso
	GG2.GP9 Evaluar objetivamente la adherencia
	GG2.GP10 Revisar el estado con los directores de alto nivel
GG3 Institucionalizar un proceso definido	GG3.GP1 Establecer un proceso definido
	GG3.GP2 Recolectar información de mejora

Tabla 12. Metas y Prácticas genéricas para cada área de proceso [CRMM10]

Ya tenemos un punto de partida para establecer las prácticas que se realizarán en la organización para de cierta medida aportar a la resiliencia operacional a partir de la resiliencia del activo software.

Como se puede ver, las áreas de proceso aplicarán de manera distinta a cada tipo de software definido, no será igual para todos los casos, por lo tanto la guía tendrá que considerar la hoja de ruta para los cuatro tipos de software que puede tener la organización. Teniendo esta visión específica de cada tipo de software y la descripción realizada es evidente que no todas las áreas de proceso aplican a cierto tipo de software, e inclusive que hay prácticas que se deben aplicar y otras sugerir, y que para cada solución habrán unos responsables y unas recomendaciones específicas, por tanto se analizaron las áreas de proceso a las cuáles aplica las áreas de proceso propuestas por CERT-RMM.

Como se indicó en el anterior capítulo, para todos los tipos de software tendremos un marco de Gestión de Riesgo RISK, que se aplicará de manera general al riesgo operacional, y con énfasis en las áreas que involucra el uso, adquisición o desarrollo de software.

Para todos los tipos se considerará el área de proceso *Definición y Gestión de Activos* ADM debido a que es el punto de partida donde se definirá la propiedad y vigilancia del software

en cuestión, de igual manera se analizarán las dependencias y se establecerá el inventario, por lo tanto se considerará en todos los casos.

De igual manera, aunque tendrán requisitos diferentes debido a que dependerá de que tan inmersa esté la organización en el desarrollo, todos los tipos deberán considerar las áreas de proceso *Desarrollo de Requisitos de Resiliencia* RRD y *Gestión de Requisitos de Resiliencia* RRM. En este considerarán requisitos de resiliencia asociados al software que a su vez soportarán y serán asignados a los servicios, que posteriormente serán gestionados.

De igual manera con base a lo que establezca la organización a nivel de control y teniendo en cuenta las referencias a COBIT que se harán más adelante, se debe tener en cuenta el área de proceso *Gestión de Controles* CTRL

En cuanto al área de proceso *Ingeniería de Soluciones Técnicas Resilientes* RTSE, es claro que sólo aplica en el caso del Software construido in-house y el Software construido por externos, pero desde perspectivas diferentes. El Software construido in-house tendrá la obligación de establecer las medidas necesarias para que el desarrollo cumpla los requisitos de resiliencia, mientras que al Software construido por externos no podemos exigirle que se desarrollen con metodologías y prácticas sugeridas–a menos que lo estipule el contrato– sino que tenemos que exigir que el software a desarrollar cumpla con los requisitos de resiliencia que establece la organización.

La continuidad del Servicio *Continuidad del Servicio* SC si es fundamental, y sobre todo considerando los riesgos operativos que implica el software, por tanto tendrá que ser considerado en todos los casos.

El área de proceso *Gestión de Dependencias Externas* EXD aplicará en todos los tipos que involucre a terceros, pero por supuesto cada tipo tendrá unas recomendaciones a la medida, debido a que no se recomendará lo mismo a un tercero al que se le debe dar acceso al servidor central de la organización que a un tercero del que dependa un servicio directamente.

Como se había indicado, el área de proceso encargada de la gestión de la protección y la gestión del riesgo, integridad y disponibilidad en los activos de tecnología, es el área de *Gestión de la Tecnología* TM por lo tanto será considerado en todos los casos.

Tipo de Software	Área de Proceso CERT-RMM asociada							
	ADM	RDD	RMM	CTRL	RTSE	SC	EXD	TM
Software construido *in-house*	X	X	X	X	X	X		X
Software construido por externos	X	X	X	X	X	X	X	X
Software adquirido	X	X	X	X		X	X	X
Software como servicio contratado	X	X	X	X		X	X	X

Tabla 13. Tipos de Software y Áreas de proceso involucradas.

Una vez clasificado, se analizará las implicaciones para cada uno de los tipos de acuerdo a las prácticas recomendadas y se sugerirán marcos de referencia y estándares que ayuden a elaborar los productos de cada práctica.

4.3 COBIT y Gestión de la Resiliencia de Software

La manera más factible que se analizó para implementar unas prácticas y recomendaciones de resiliencia de software es sobre el proceso de TM *Gestión de la Tecnología,* como se indicó en el anterior apartado, debido a las relaciones en áreas de proceso que tuvo en cuenta el CERT-RMM. De este modo, es importante que basado en el marco de gestión de TI que siga la organización se tengan en cuenta las prácticas necesarias para llevar a cabo la gestión de la resiliencia, y así poder asignar responsables a cada una de las prácticas propuestas.

Antes de establecer estas relaciones, se realizará una breve contextualización del marco de control COBIT en su versión 5, pues en este marco tenemos una mayor convergencia entre la gobernanza de TI, la gestión de TI, la gestión de riesgos, la gestión de la seguridad de la información y la gestión de servicios de TI.

COBIT 5 define un marco para el gobierno y la gestión de las TI de la empresa, pero también dentro de su familia de productos publica la implementación y una guía de catalizadores de COBIT 5, en las que se discuten en detalle los catalizadores para el gobierno y gestión.

El marco COBIT 5 [COBIT5] se construye sobre cinco principios básicos:

- ✓ **Principio 1. Satisfacer las Necesidades de las Partes Interesadas.** Establece la importancia de la creación de valor en las organizaciones, así como la relación entre beneficios, optimización de riesgos y uso de recursos. Y es el aporte que da COBIT 5

a través de la definición de los procesos y catalizadores que permiten que se aporte valor al negocio mediante TI.

- ✓ **Principio 2: Cubrir la Empresa Extremo-a-Extremo.** COBIT 5 considera la integración del gobierno y la gestión de TI en el gobierno corporativo, pues realiza el cubrimiento de las funciones y procesos de la organización –no solo en la función de TI, además propone los catalizadores a nivel de toda la empresa.

- ✓ **Principio 3: Aplicar un Marco de Referencia único integrado.** La alineación de COBIT con otros estándares y marcos de trabajo es muy importante, pues le da ese aporte a las propuestas que establece como prácticas, y le da una visión integrada.

- ✓ **Principio 4: Hacer Posible un Enfoque Holístico.** Para mantener el enfoque holístico, COBIT 5 define un conjunto de catalizadores (*enablers*) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Estos catalizadores son aportes para la consecución de las metas de la empresa, y son definidos en siete categorías (Principios, Políticas y Marcos de Trabajo, Procesos, Estructuras Organizativas, Cultura, Ética y Comportamiento, Información, Servicios, Infraestructuras y Aplicaciones, Personas, Habilidades y Competencias).

- **Principio 5: Separar el Gobierno de la Gestión.** Como se había indicado en el estado del arte, es necesario entender la diferencia que hay entre gobierno y gestión, pues cada una tiene diferentes metas, actividades y responsables. COBIT 5 establece:
  - **Gobierno.** "El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas" [COBIT5].

El gobierno es responsabilidad del comité de dirección bajo el liderazgo del presidente, aunque hay algunas responsabilidades que se pueden delegar dependiendo de la complejidad de la organización.

- **Gestión.** "La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales". [COBIT5]

  La gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO).

El objeto de este trabajo no es el estudio al detalle de COBIT 5, sin embargo si es nuestro objetivo basarnos en un marco que nos oriente en la aplicación de la gestión de la resiliencia software dentro de un entorno de empresa, utilizaremos COBIT 5 como referente para relacionar las metas corporativas que implica la resiliencia organizacional con las metas de TI, y poderlo relacionar con los procesos, estos nos servirá de orientación para relacionar las prácticas de resiliencia para cada tipo de software que se indicaron anteriormente.

La organización primero debería plantearse qué le motiva a establecer resiliencia operacional y específicamente resiliencia de software en la organización. En nuestro caso tomaremos que el gobierno y la gestión considera las siguientes preguntas: ¿He contemplado todos los riesgos relacionados con TI? ¿Estoy ejecutando una operación de TI eficiente y robusta? ¿Cómo es de crítica la TI para para la sostenibilidad de la empresa? ¿Qué pasaría si la TI no estuviera disponible? Estas preguntas nos relacionarían con al menos tres de las metas corporativas que se establece, sin embargo nos centraremos en una que es común y que nos lleva a uno de los objetivos de la resiliencia operacional y específicamente la relacionada con tecnología, "Continuidad y disponibilidad del servicio de negocio", y esto justificado que se busca garantizar la operación del servicio en condiciones de estrés o interrupción.

En la Tabla 14 se encuentran las metas corporativas que relaciona COBIT. Se subrayó en amarillo la que se relaciona con la "continuidad y disponibilidad del servicio de negocio". En rojo se subrayaron las metas relacionadas con TI asociadas a la meta corporativa de nuestro interés.

Si analizamos estas metas, tienen una estrecha relación con el planteamiento inicial de la resiliencia operacional hecha en CERT-RMM, y podrían ser mapeadas a la hora de establecer la guía en la organización:

- **Alineamiento de TI y la estrategia de negocio** (Secundario). Como se pudo ver, concuerda con el CERT-RMM específicamente en el planteamiento de las metas generales. Es necesaria la alineación de TI y negocio como punto de partida para el establecimiento de la resiliencia operacional.
- **Riesgos de negocio relacionados con las TI gestionados** (Primario). Es fundamental tener en cuenta un marco de gestión de riesgos. También concuerda con CERT-RMM.
- **Entrega de servicios de TI de acuerdo a los requisitos del negocio** (Secundario). La gestión de servicios se debe tener en cuenta para lograr esta meta corporativa, y también concuerda con CERT-RMM.
- **Uso adecuado de aplicaciones, información y soluciones tecnológicas** (Secundario) Esta corresponde directamente a la gestión de TI, es decir que también tiene concordancia con CERT-RMM.
- **Seguridad de la información, infraestructuras de procesamiento y aplicaciones** (Primario) La gestión de la seguridad es uno de los pilares del planteamiento de la resiliencia operacional para CERT-RMM

			Meta corporativa																
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activo)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Tabla 14. Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI [COBIT5] Resaltado por Autor[16]

[16] 'P' para principal, cuando hay una importante relación, es decir, las metas relacionadas con TI que son el pilar imprescindible para conseguir los objetivos de la empresa. – 'S' para secundario, cuando todavía hay un vínculo fuerte, pero menos importante, es decir, las metas relacionadas con TI son un soporte secundario para los objetivos de la empresa.

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5						Financiera				Cliente				Interna				Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			

Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

Tabla 15. Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos [COBIT5] Resaltado por Autor

- **Disponibilidad de información útil y relevante para la toma de decisiones** (Primario). Esta meta considera la importancia del gobierno sobre esta meta relacionada a TI, pues le dará las herramientas (métricas, seguimiento, informes) de la eficacia de las medidas sobre la continuidad y disponibilidad, y en contexto las medidas en resiliencia operacional.

Podríamos ir mucho más al detalle, y ver cómo se relacionan estas metas relacionadas con TI y mapearlas con los procesos COBIT a los cuales referencia. En la Tabla 15 se subrayaron las metas de COBIT que relacionamos y se puede ver que hay un número

considerable de procesos que se relacionan con la continuidad y disponibilidad del servicio de negocio.

Debido a que este estudio no tiene como fin establecer los procesos relacionados con la gestión de la resiliencia operacional en general, sino específicamente aquellos procesos que involucren la gestión de la resiliencia de software considerando los tipos de software planteados, no se observará al detalle cada proceso que esté mapeado con las áreas en general. El objetivo tampoco es establecer una metodología para el manejo de la resiliencia software en la organización basado en la gestión de TI, lo que se quiere resaltar es la relación que establece la gobernanza y gestión de TI con la gestión de la resiliencia software.

En la tabla 16 se relacionaron procesos COBIT con las metas de TI que fueron seleccionadas, y se realizó una breve justificación de su relación con la resiliencia software. Los procesos EDM se relacionan con el Gobierno de TI, el resto con la Gestión de TI.

Proceso COBIT	Justificación
EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	Es la primera estancia para el establecimiento de la gestión de la resiliencia operacional, por lo tanto aplica para la gestión de la resiliencia software. Se relaciona con metas 1 y 7.
EDM02 Asegurar la Entrega de Beneficios	Asegurar que se obtendrán beneficios de la inversión en resiliencia software. Se relaciona con metas 1 y 7.
EDM03 Asegurar la Optimización del Riesgo	El entendimiento de la tolerancia, apetito de riesgo que acepta la organización en cuanto a servicios basados en software y en la gestión de los riesgos operacionales. Se relaciona con metas 4 y 10.
EDM05 Asegurar la Transparencia hacia las Partes Interesadas	Las métricas que se presenten para informar la eficacia de la implantación de la resiliencia deben contar con la transparencia y conformidad. Se relaciona con meta 7.
AP009 Gestionar los acuerdos de servicio	Es necesaria la identificación de los servicios de TI, y hacer la valoración de los mismos, para identificar los de alto valor y que estén relacionados con el software. Del mismo modo será necesario evaluar los niveles de servicio con las necesidades y expectativas de la empresa. Se relaciona con metas 7 y 14.
APO10 Gestionar los Proveedores	Es necesario que se administren los servicios de TI prestados por todo tipo de proveedores para soportar las necesidades del negocio. Por lo tanto se debe tener en cuenta la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y

	cumplimiento adecuados. Se relaciona con metas 4 y 7.
APO12 Gestionar el Riesgo	Como se indicaba anteriormente, es vital para la resiliencia identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Se relaciona con metas 4 y 10.
BAI03 Gestionar la Identificación y Construcción de Soluciones	Este proceso es el que se ve relacionado de manera directa con la gestión de la resiliencia software, pues la descripción define "Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios." Se relaciona con meta 7. En este apartado hay prácticas específicas relacionadas con la construcción, verificación, calidad, requisitos, que pueden aportar a los tipos de software desarrollados *in-house*.
BAI04 Gestionar la Disponibilidad y la Capacidad	La importancia de este proceso es que establece la evaluación de la disponibilidad actual, y el impacto sobre el negocio. Se relaciona con metas 7 y 14.
BAI09 Gestionar los Activos	A pesar que no está relacionado dentro de las metas, en nuestro caso la resiliencia debe considerar el activo software para clasificarlo, no todo el software es de alto valor para la organización y no todo software de alto valor para la organización está estrechamente relacionado a un servicio de alto valor.
DSS01 Gestionar Operaciones	La gestión de las operaciones se puede relacionar con los procedimientos tanto internos como externos para entrega de los servicios de TI. Se relaciona con metas 4 y 7.
DSS04 Gestionar la Continuidad	La gestión de la continuidad es vital, pues no podemos hacer resiliente al software de cualquier amenaza, por lo tanto hay que tener en cuenta la continuidad en caso que se presente una interrupción.

Tabla 16. Procesos de COBIT 5 [COBIT5] relacionados con Resiliencia Software.

Basado en estos procesos se podrían gestionar las prácticas relacionadas y se podrá establecer la gestión de la resiliencia del software que aporte a las metas de TI y a la vez a la meta de la gestión corporativa. Del mismo modo basado en COBIT podemos asignar responsabilidades sobre cada uno de los procesos que soporta la implantación de la resiliencia del software en la organización.

5. RESULTADOS

5.1¿A quién va dirigida la Guía?

La guía va dirigida a todos aquellos interesados en el activo software durante su ciclo de vida, y a aquellos con responsabilidad en la seguridad y continuidad de los servicios en la organización.

Esta guía será utilizada por la dirección para saber cómo el software se mantendrá disponible e íntegro para la operación de los servicios. También será suministro de información de rendimiento para los ejecutivos en el proceso de aseguramiento de la consecución de la misión de la organización frente a amenazas, a través de las TI y específicamente de aquellos servicios que sean basados en software. La cartera proyectos de tecnología lo tendrá como referencia para saber cómo relacionar el proyecto de TI con la estrategia de la organización y qué prácticas seguir para implantar la resiliencia en los proyectos. Los equipos de construcción, personal de seguridad y continuidad, así como los de gestión de riesgos tendrán la tarea de coordinar sus actividades de acuerdo a la guía con el fin de ofrecer servicios resilientes. El equipo de adquisición o contrato, tendrá que tener en cuenta las condiciones que debe cumplir el proveedor de servicios de modo que se mantengan las estrategias de resiliencia operacional con base en el software adquirido o contratado. Los terceros deberán ser conscientes de la estrategia que establezca la organización para mantener operativos sus servicios y comprometerse a través de los contratos o SLA.

5.2 Propósito de la Guía

La guía será una ayuda para implementar la resiliencia en el software, como para los procesos que implica la construcción, adquisición o contrato del mismo, en un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores prácticas, de modo que se asegure la resiliencia operacional de los servicios que soporte el software, a través de estrategias de seguridad y continuidad.

Esta guía de mejores prácticas tiene como referencia el modelo CERT-RMM (CERT *Resilience Management Model*) que establece una gestión de resiliencia operacional en ambientes complejos y con riesgo de evolución. Traza con los procesos COBIT para

establecerlo en un marco de Gestión de TI que apoye la Gobernanza de TI, e incluye estándares que soportan tanto la gestión de los servicios de TI, como la gestión de la seguridad informática y de la continuidad del negocio.

5.3 Beneficios implantar la guía en la Organización

- La guía aporta resiliencia en el software y los servicios que el software soporta. Garantía en las soluciones software en cuanto a disponibilidad e integridad.
- Consideración durante todo el ciclo de vida del software de mejores prácticas en seguridad y continuidad.
- Motiva a la organización a establecer un esfuerzo coordinado en las prácticas para el control y sostenimiento del activo, con el fin de garantizar el éxito en el proceso de negocio, en el servicio, y por ende en la misión de la organización.
- Incentiva el análisis costo beneficio en la implantación de soluciones y puede reducir los costos de la gestión de riesgos.
- Propone prácticas de monitorización y seguimiento durante la implantación.

5.4Aplicaciones de la Guía

La creciente tecno-dependencia en las organizaciones, y los servicios que soporta el software –siendo actualmente el software uno de los eslabones más vulnerables a amenazas en la organización– la guía es un aporte para garantizar que se realizan las mejores prácticas de resiliencia que le garantiza a la organización la protección y sostenibilidad del software y los servicios que este soporte.

Es aplicable si se necesita establecer mejores prácticas en ciberseguridad, si se tiene por objeto garantizar mejores prácticas de seguridad durante el ciclo de vida del software y a la vez establecer un “blindaje” a los servicios que soporte y una capacidad no solo reactiva sino proactiva a amenazas de seguridad.

Contribuye de manera significativa en un entorno empresarial el cual se base en estructuras complejas debido al trabajo con terceros, tanto para la construcción, adquisición y contrato de software, pues su base es el modelo CERT-RMM que considera estas relaciones y entornos cambiantes de riesgos.

5.5 Entorno de Implantación

Una vez conocidas las áreas de conocimiento que involucra la resiliencia operacional aplicado a un entorno operacional, justificando como traza para el beneficio de la organización teniendo en cuenta la gobernanza corporativa, gobernanza corporativa de TI, la gestión de la seguridad y la continuidad, se plantea un entorno de implantación como referencia el cual se desarrolla no solo teniendo en cuenta la "convergencia" propuesta por el CERT-RMM sino también las Disciplinas de Thorpe, orientando al usuario para que visualice el entorno de aplicación, y con la información suministrada escoger los estándares y las mejores prácticas que considere oportunas –Aunque en este estudio se sugiere la mayoría– para implementar en cada una de las capas.

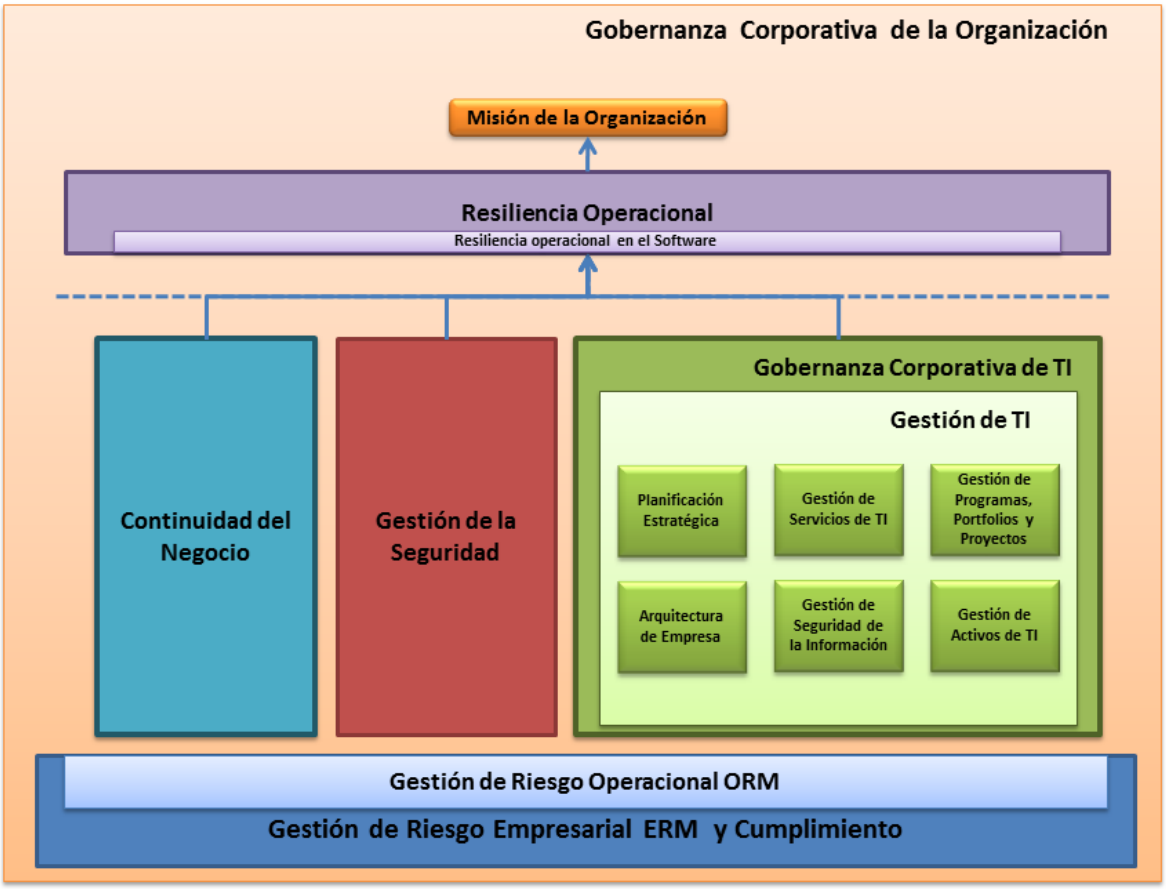

Figura 21. Entorno de implantación de la Guía

5.6 Guía de Implantación de Resiliencia en el Software de un Entorno Operacional de una Organización, con base en Estándares, Modelos y Mejores prácticas

Teniendo en cuenta un marco de Gestión de TI como COBIT, que nos da una idea del aporte de la resiliencia software en los procesos de gestión de TI, y del mismo modo conocer el aporte de la resiliencia operacional a los nuevos ambientes más complejos de riesgos, y entrando a fondo en un modelo que nos traza un camino sobre la consideración de la resiliencia operacional en las organizaciones, el resultado de este trabajo es una guía que pretende establecer unas recomendaciones basadas en las prácticas que establece el CERT–RMM para considerar la resiliencia del software en la organización.

La guía consiste en una matriz que contiene las áreas de procesos relacionadas con la resiliencia operacional, aplicada para cada uno de los casos, y estas a su vez con las metas y prácticas asociadas basadas en el modelo CERT-RMM. Sobre estas prácticas se realizarán una serie de recomendaciones que le permitirá al gestor de la resiliencia seguir cada una de las prácticas con las recomendaciones indicadas. Estas recomendaciones se basarán tanto en el análisis del CERT-RMM y se complementará con diferentes marcos de referencia, estándares y mejores prácticas, haciendo énfasis en la importancia y producto de la aplicación de la práctica.

Es importante hacer énfasis que el área de proceso RTSE, de uso en software construido in-house, y guía para el desarrollo de soluciones técnicas por terceros, debe ser sugerida o acordada en los contratos o debe ser un factor para la decisión en los procesos de contrato, tanto para soluciones empaquetadas o de tipo Cloud. Como se podrá observar es específicamente la que aporta mucho más a la resiliencia del software como tal a nivel técnico.

Cabe resaltar también que en todas las áreas de proceso aplicarán las metas genéricas de la Tabla 12.

5.1.1 Software construido in-house

Área de Proceso	Metas	Prácticas	Recomendaciones
ADM	ADM:SG1	ADM:SG1.SP1	**Inventario de Activos** Es importante para la organización mantener de manera organizada sus activos, y del mismo modo se espera que la organización siga unas mejores prácticas en cuanto a la gestión de los mismos. Debido a que tratamos con software se debe tener en cuenta que al ser un activo intangible relacionado con tecnología, no tendrá un manejo igual al que tendrá un activo físico. De esta manera la gestión de TI debe asegurarse de establecer una adecuada gestión de activos de TI para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios, todo esto alineado con el marco de gobernanza de TI. En el caso del software construido in-house, se deben considerar varias situaciones, por ejemplo que hace parte del capital intelectual de la empresa, que dependerá de otros activos y que en general debe tenerse una práctica adecuada que soporte la actividad. Un concepto importante es *Software Asset Management* (SAM), que corresponde a que a nivel de negocio se realice una adecuada gestión de la adquisición, mantenimiento, uso y disposición de las aplicaciones software dentro de la organización y la optimización de los procesos que se gestionan. Se sugiere utilizar marcos de gestión de software como ISO/IEC 19770 que se complementa con ISO 20000 en el proceso Gestión de la Configuración y en la cual la organización puede demostrar que realiza una gestión de activos de software. De igual manera ITILv3 incluye el proceso de Activos de Servicio y Gestión de la Configuración. COBIT 5 está alineado con ITILv3, por lo tanto puede considerar el inventario a alto nivel en la gestión de TI. Del mismo modo, SAM aporta a ISO/IEC 27002, en lo que a incidentes de seguridad de Software considera, es por esto que será un control preventivo a situaciones de interrupción o estrés. El producto de esta práctica debe ser un inventario y una base de datos del software de la organización. Del mismo modo se deberá identificar cuál software que se produce soporta procesos críticos del negocio y son vitales para la operación y la consecución de los objetivos de la organización. Se establecerá el valor de cada software que se produzca.
		ADM:SG1.SP2	**Establecer un Entendimiento Común** Es importante que se clasifiquen los activos software dentro de los activos de tecnología, del mismo modo, usando uno de los marcos sugeridos en ADM:SG1.SP1 se tendrá una buena práctica para que se manejen los activos de manera adecuada, y podrá ser el punto de partida para que se puedan asignar tanto a propietarios como vigilantes y entiendan sus responsabilidades (en la siguiente práctica ADM:SG1.SP3). El entendimiento será un punto de partida para evaluar las prioridades sobre los activos software en cuanto a resiliencia operacional, para saber cuáles tienen mayor valor para la organización en cuanto a resiliencia operacional no solo porque sean activos de alto valor sino también por los servicios que soporten, cuáles soportan servicios críticos y a partir de esto dará un enfoque global para establecer los requisitos de resiliencia. Un entendimiento claro a nivel interno, garantiza que las personas relacionadas con el producto software construido en la organización tengan la conciencia no solo de las responsabilidades sino en las prioridades en cuanto a servicios, de este modo será una entrada para establecer responsables y los requisitos de resiliencia. A través de esta práctica se llegará al entendimiento de los activos software y sobre todo cuáles son los de mayor importancia por soportar los servicios de la organización. Esto se puede realizar documentando la información necesaria, como políticas de uso, importancia y concienciación del activo frente a los servicios, entre otros.
		ADM:SG1.SP3	**Establecer Propietarios y Vigilantes** El software, como el resto de activos, tendrá asociados unos propietarios y unos vigilantes. Establecer mejores prácticas ADM:SG1.SP1 en general sobre los activos, y con un entendimiento común ADM:SG1.SP2 del aporte del software a la organización hará mucho más fácil establecer quién es quién dentro de las funciones del activo, y del mismo modo establecerá las pautas para la resiliencia operacional de la organización. Por un lado se establecerán los propietarios que tendrán la responsabilidad de la viabilidad, productividad y resiliencia del software, no necesariamente serán personas directamente, pueden ser unidades organizacionales internas debido a que el software es construido in-house. Por otro lado se establecerán vigilantes –que también serán

			personas o unidades organizacionales internas– con la responsabilidad de implementar y gestionar los controles para satisfacer los requisitos de resiliencia, mientras estén a cargo del activo. Cabe resaltar que como se indicó anteriormente, en todos los casos, los propietarios son los responsables de asegurar la protección y continuidad apropiada de sus activos, sin tener en cuenta las acciones (o inacciones) de los vigilantes. El resultado de esta práctica será la identificación de los propietarios y los vigilantes y la actualización de los perfiles y las bases de datos de activos definidos. Es importante definir el perfil de propietario y vigilante y las responsabilidades que tienen con el software. En caso que el software soporte junto a un grupo de activos un servicio de la organización, es necesario establecer este grupo dentro de la identificación.
	ADM:SG2	**ADM:SG2.SP1**	**Asociar Activos con Servicios** Una práctica muy importante es empezar a establecer la relación de los activos con los servicios de la organización. Para una organización, asociar activos con los servicios es una práctica muy significativa debido a que es mucho más importante establecer resiliencia en un servicio de alto valor, que en un servicio complementario. La resiliencia operacional busca que la organización se enfoque en la visión de los servicios, debido a esto asociará el activo al servicio que soporta. En el caso del software, se tendrá clara no solo cuál será la funcionalidad y el para qué se construye, sino que se sabrá cuáles servicios van a asociarse y cuál será su rol para soportar el servicio. A partir de esta definición, será más fácil establecer las mejores estrategias en cuanto a protección y sostenimiento del software. Como resultado de esta práctica tendremos qué software se relaciona a los servicios de alto valor de la organización.
		ADM:SG2.SP2	**Analizar dependencias entre activos y servicios** Un activo puede soportar uno o más servicios, por esto se debe realizar un análisis general de estos servicios en la organización. Un CRM por ejemplo puede soportar varios servicios de la organización, y del funcionamiento de este podrán verse afectados uno o más servicios de alto valor. Una buena identificación de las dependencias es crucial pues será base para el establecimiento de los requisitos de resiliencia y por ende la estrategia de protección y sostenimiento del software. Como resultado de esta práctica evitaremos los conflictos potenciales por dependencias entre activos y se establecerán acciones y soluciones de mitigación.
	ADM:SG3	**ADM:SG3.SP1**	**Identificar Criterios de Cambios** (Esta práctica será complementaria a RRM:SG1.SP3) El ajuste a las necesidades de la organización y específicamente a los requisitos de resiliencia, afectará de manera directa al activo o a la asociación que tenga con un servicio, es por esto que se debe tener una práctica que sirva de soporte para el establecimiento y mantenimiento de los cambios. Los cambios identificados pueden afectar a uno o más activos, por esto las prácticas anteriores deberán soportar la estrategia de gestión del cambio establecida por la organización. Para este caso, la construcción del software implicará directamente el proceso, por lo tanto habrán factores esenciales que tendrán que ser manejados y que podrían implicar cambios (requisitos nuevos, cambio de infraestructura y configuración, cambio de staff, caminos alternativos,…). Los propietarios serán directamente capaces de establecer la aplicación y gestión de los cambios sobre el software. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
		ADM:SG3.SP2	**Mantener Cambios a los Activos e Inventarios** (Esta práctica será complementaria a RRM:SG1.SP3) Así como se identifican los cambios, es necesario gestionarlos de manera adecuada, teniendo en cuenta los marcos de referencia que utilice la organización para el mantenimiento de cambios. Hay diferentes condiciones que enfrentan a realizar cambios en el proceso de construcción de software, es importante gestionar estos cambios y lograr un entendimiento amplio de modo que estos cambios no afecten de manera total el servicio que soporta. Esta práctica pretende que haya procedimientos documentados de la gestión de cambios en el activo y que se tenga presente el estado del activo en ciertos instantes, de acorde a esto establecer los requisitos de resiliencia y la estrategia de protección y sostenimiento del software y de los servicios que soportan. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
RISK	**RISK:SG1**	**RISK:SG1.SP1**	**Determinar las categorías y fuentes de Riesgo** Es necesario que se establezcan las fuentes de riesgo a las que se va a exponer el software, no solo como producto sino como proceso, y a partir de esto establecer las

			categorías y una taxonomía del riesgo operacional, que es el que implica directamente la operación habitual de los servicios. Identificar el riesgo es comprender a qué se enfrentará el software, y a pesar de no poder contar con todos los escenarios posibles ni blindar la operación a todas las amenazas, lo más importante es identificar lo más crítico y considerar los *Black Swan.* Hay que considerar las fuentes tanto internas como externas. La organización debe establecer un marco para la gestión de riesgos que tenga una visión holística del software, como se indicó en el Capítulo 2 seguir un estándar como ISO 31000 junto con mejores prácticas para el ciclo de vida del software (no solo del producto sino del proceso) nos ayudará a establecer lo que se espera de esta práctica, el riesgo operacional al que se expone el software, las categorías de riesgo y la taxonomía. Este marco de referencia será el apoyo para la definición de los requisitos de resiliencia.
		RISK:SG1.SP2	**Establecer una estrategia para la Gestión de Riesgo Operacional** La organización que cuenta con un marco para la gestión del riesgo empresarial ERM, generalmente cuenta con la base necesaria para establecer la gestión de riesgo operacional ORM. De acuerdo como decida la organización su estrategia a nivel ejecutivo, decidirá cuál será la estrategia a seguir para la ORM que cumpla con los objetivos del negocio. La estrategia que se establezca será la que defina el desarrollo de las actividades relacionadas con la ORM y la colección, coordinación y gestión de dichos riesgos al marco de procesos de ERM. Dentro de la estrategia se debe contar con que el software se construye in-house, por lo tanto la construcción y el mantenimiento del software será responsabilidad de la organización. La estrategia debe estar documentada y comunicada a todos los interesados internos y externos responsables de las actividades de ORM, de modo que se tenga el entendimiento y sirva de entrada para otros procesos –por ejemplo para definir los requisitos de resiliencia.
	RISK:SG2	**RISK:SG2.SP1**	**Definir los parámetros de Riesgo** Para evaluar la relevancia del riesgo operacional en la organización, es preciso establecer unos parámetros con los cuales se pueda medir, es decir, se tenga una fotografía del estado actual de la organización. Para esto se definirán unos umbrales de tolerancia de riesgo que reflejará el nivel de riesgo dispuesto a admitir y a enfrentar la organización. Este deberá considerar que el riesgo implicará el proceso y el producto y que toda la gestión será por parte de la organización. Con un marco de gestión de riesgos, es claro que se establecerán estas medidas, y que acorde a la estrategia y objetivos de la organización se dictarán los parámetros a los que quiere apuntar y con los que evaluará el riesgo operacional, y con los cuáles definirá los requisitos para la gestión de riesgos.
		RISK:SG2.SP2	**Establecer criterios de medida del riesgo** Así como se definen los parámetros, es necesario definir los criterios para medir el impacto del riesgo dentro de la organización. Estos criterios serán importantes para clasificar, evaluar y priorizar los riesgos operacionales. El producto de esta práctica es el conocimiento de las áreas de impacto –donde el riesgo material tiene consecuencias significativas e interruptivas– priorización de dichas áreas y un documento con los criterios de medida y evaluación y con la probabilidad de riesgos.
	RISK:SG3	**RISK:SG3.SP1**	**Identificar los Niveles de riesgo en los Activos** Antes de establecer resiliencia operacional sobre los activos, es preciso que se tenga claro que los activos y por ende servicios se pueden ver afectados por los riesgos operacionales, por lo tanto su identificación y mitigación es primordial. Acorde a las categorías y al nivel de riesgo definidos por la organización, se identificarán los riesgos que afecten a los activos, en este caso al software. Eso sí, es claro que no se identificará la totalidad de riesgos, pero al menos los riesgos operacionales que afecten los servicios, estos deben ser identificados y gestionados a través de diferentes técnicas. De ahí la importancia de seguir uno de los marcos para la gestión de riesgos. Deberá considerarse los escenarios en los cuales la gestión sea por parte de la organización, tanto en la construcción como en la función. Como producto de esta práctica, tendremos un conjunto de herramientas para la identificación del riesgo organizacional, y una lista de riesgos categorizados por activo.
		RISK:SG3.SP2	**Identificar los Niveles de riesgo en los Servicios** El objeto de establecer la resiliencia operacional, es garantizar que los servicios cumplan la misión, sin embargo estos servicios están expuestos a unos riesgos operacionales que son el resultado de una serie de riesgos sobre los activos de la organización. Por esta razón hay que evaluarse el impacto potencial de un riesgo sobre un activo, en este caso los riesgos sobre el producto software y el proceso de construcción y funcionamiento, y su impacto sobre la misión del servicio. De acuerdo a esto no solo se puede mitigar sino priorizar teniendo en cuenta los intereses de la organización. Se asume que la organización identificó de manera esencial los servicios de alto valor, y en el proceso ADM los activos asociados a estos servicios.

			Como resultado de esto podremos clasificar los riesgos por servicio y establecer contextos donde afecta el servicio y consecuencias de los riesgos sobre los servicios si se llegan a materializar.
	RISK:SG4	**RISK:SG4.SP1**	**Evaluar Riesgos** Teniendo como lineamiento las prácticas realizadas anteriormente para la medición del riesgo (tolerancia, criterios e impactos del riesgo), lo siguiente es evaluar el riesgo operacional y sus consecuencias. Los riesgos varían en cada caso y específicamente para el software tenemos que considerar los diversos escenarios a los cuales esté expuesto el proceso. Esta evaluación nos dará una idea de cómo manejaremos el impacto de los riesgos y cómo actuar en diversas circunstancias operativas. El producto de esta práctica será la evaluación con base a los lineamientos de la organización y darle un valor cualitativo para poder decidir cómo actuar, y cómo priorizarlos.
		RISK:SG4.SP2	**Categorizar y Priorizar Riesgos** Una vez evaluados, podemos categorizar los riesgos operacionales de modo que establezcamos las prioridades sobre las actuaciones que se vayan a realizar sobre los mismos. Las categorías dependerán de los intereses, pero hay diferentes maneras de categorizas, por fuentes, por nivel de riesgo, por taxonomía, etc. Es importante tener en cuenta los escenarios y no olvidar los *Black Swan*, que en muchos casos son causas drásticas de interrupción o estrés del servicio. La priorización será importante a la hora de establecer resiliencia. Como resultado de esta práctica tendremos los riesgos por categorías y con priorización, de acuerdo a los intereses de la organización.
		RISK:SG4.SP3	**Asignar disposición al Riesgo** Del mismo modo que la organización asume que hay entendimiento de los riesgos, puesto que de acuerdo a su postura se evalúa, tiene también que documentar y aprobar su posición frente a los escenarios de riesgo identificados. Las acciones que tome de acuerdo a los riesgos tendrán que ser el producto de la estrategia establecida en la gestión de riesgos. La organización puede tomar diferentes disposiciones, entre ellas evitar el riesgo, aceptar el riesgo, transferir el riesgo o mitigar y controlar. Como producto de esta práctica de deberá listar los riesgos y la disposición de la organización, y los riesgos priorizados para mitigar. La disposición al riesgo será documentada y debidamente aprobada por la organización (en especial con los riesgos que se aceptarán).
	RISK:SG5	**RISK:SG5.SP1**	**Desarrollar planes para la mitigación del riesgo** Es necesario que se desarrollen planes de mitigación, sobre todo cuando el riesgo, producto de la evaluación realizada, está sobre el umbral y es inaceptable de admitir, no se desea transferir, y evitar solo sea posible eliminando la actividad que lo genera. La mitigación del riesgo puede requerir actividades referentes a la protección y sostenimiento del activo, o en algunos casos implementación de controles. En algunos casos las actividades no son suficientes y se deberá considerar el riesgo residual. Como práctica resultante tendremos el plan de mitigación del riesgo, para todos los riesgos a los que se dispuso mitigar y controlar. En este plan debe estar claro cómo se reduce la amenaza o cómo se protege la vulnerabilidad, las acciones preventivas, los controles a implementar, los planes de continuidad del servicio y los responsables del mismo, el costo del plan, manejo del riesgo residual.
		RISK:SG5.SP2	**Implementar estrategias de Riesgo** La organización toma una posición frente a los riesgos, y se espera que las estrategias que establece en la gestión de riesgos se sigan durante el todo el proceso, es por esto que los planes y estrategias de mitigación de riesgos serán implementados y además monitorizados. Lo que se gana con este ciclo continuo es que en un entorno cambiante de riesgos, debido a las nuevas condiciones de complejidad que se ve en las organizaciones de hoy en día, se tenga claro que la estrategia esté bien dirigida y los riesgos bien identificados, y en caso de cambios se revise y se modifique. El producto de esta práctica será la documentación de la implementación del plan de mitigación, y una visión actualizada del estado de los riesgos de acuerdo a la efectividad de la mitigación frente a las condiciones actuales, a través de la monitorización y unas políticas de seguimiento.
	RISK:SG6	**RISK:SG6.SP1**	**Revisar y ajustar estrategias para proteger los activos y servicios** Una de las formas de gestionar el riesgo operacional es la protección de activos y servicios, por lo tanto los controles que se implementen con este fin deben ser evaluados constantemente y actualizados según se requiera con base en la información que proporcione el riesgo. Los controles serán el resultado del proceso de gestión de riesgo o de los requisitos de resiliencia, la experiencia de la organización es la que le dará la madurez de la definición de estos controles, mejorar los actuales e implementar los que necesite, así como la consideración de controles que podrán proteger los activos y servicios de

			situaciones de riesgo emergentes. El producto de esta práctica será la lista de controles a revisar, mejorar o desarrollar y un plan de revisión.
		RISK:SG6.SP2	**Revisar y ajustar estrategias para sostener los activos y servicios** La otra forma de gestionar el riesgo operacional es el sostenimiento de activos y servicios, por lo tanto las estrategias de continuidad del servicio serán fundamentales de acuerdo al análisis que se realice en caso que el riesgo se materialice. Para esto se plantean planes de continuidad del servicio. Basado en la información de riesgo y lo aprendido en el ciclo de vida del riesgo, se pueden identificar falencias en la definición de los planes a través de las revisiones y posteriormente proponer mejoras. La validación de los planes será una manera de saber su efectividad frente a riesgos o amenazas operacionales El producto de esta práctica será la lista de planes de continuidad del servicio a revisar, mejorar o desarrollar y un plan de revisión.
RDD	**RRD:SG1**	**RRD:SG1.SP1**	**Establecer Requisitos de Resiliencia Empresarial** La organización a nivel de empresa, debe definir los requisitos de resiliencia con base a lo que necesite, generalmente motivados por la estrategia o cuestiones de cumplimiento. Debido a que el software es un activo de tipo "tecnología", los requisitos que se tendrán en cuenta son los que están ligados a la integridad y disponibilidad, si hace parte de un grupo de activos podrá también considerarse la confidencialidad. Como producto de esta práctica tenemos la lista de requisitos de resiliencia que define la empresa, que son el producto de la estrategia, objetivos, leyes, reglas y políticas, y serán suministrados al equipo de desarrollo, implementación y mantenimiento.
	RRD:SG2	**RRD:SG2.SP1**	**Establecer Requisitos de Resiliencia de Activos** Una vez teniendo conciencia de los requisitos de empresa con los que se verá afectado el software, se tendrá que tener en cuenta como tal los requisitos de resiliencia que conciernen directamente al software. Es claro que estos requisitos se definirán con base en los servicios de alto valor que desee proteger y sostener la organización y por ende al activo que lo soporte, que para este caso es el software. Por tanto en esta práctica se deberá hacer una lista de lo que se considera en la organización como servicio de alto valor, establecer las relaciones entre servicios, procesos de negocio y para este caso específico el software asociado, y la lista de requisitos de resiliencia por cada software de la organización que esté asociado con un servicio de alto valor. Ya que hablamos de software, es importante que se realice una buena práctica para la ingeniería de requisitos, de modo que el software que se construya con los lineamientos necesarios, del mismo modo, que el proceso de construcción también cuente con las garantías para mantener la resiliencia operacional de la organización. Teniendo ya asociados unos propietarios (proceso ADM) y con buena parte de la evaluación de riesgos (RISK), esta identificación tiene una entrada de información significativa
		RRD:SG2.SP2	**Asignar Requisitos de Resiliencia Empresarial a los Servicios** Los requisitos de resiliencia que afectan los servicios deberán ser asignados a los servicios. Aquí se establecerá la relación necesaria para identificar la colección de requisitos de resiliencia para los servicios, a través de la asociación entre misión de empresa-misión de servicio-activo asociado. El producto de esta práctica es asociada a la lista de RRD:SG1.SP1y RRD:SG1.SP2 y tendrá en cuenta los servicios relevantes junto con los requisitos de resiliencia específicos por servicio. Con esto se identifica y asignan los requisitos aplicables bajo la relación requisito empresa -requisito de servicio-requisito de activo. Esto será de gran ayuda para establecer la relación del activo software con los requisitos de los servicios y la estrategia de resiliencia operacional de la organización.
	RRD:SG3	**RRD:SG3.SP1**	**Establecer una definición de la funcionalidad requerida** La organización debe tener definidas las funcionalidades requeridas de un activo en el contexto del servicio, por lo tanto es tener clara la funcionalidad que el software va a proporcionarle al servicio de la organización y cómo se va a mantener el software a través del ciclo de vida. Realizar una monitorización de esto proporciona una entrada para el análisis y validación de los requisitos de resiliencia a nivel de activo. Esta hace parte de la descripción del activo que se hará en ADM y estará documentada.
		RRD:SG3.SP2	**Analizar Requisitos de Resiliencia** Es claro que los requisitos de resiliencia buscan proteger y sostener los servicios, sin embargo también es de resaltar que en una organización hay requisitos que dependen de otros requisitos, o que tal vez un requisito entre en conflicto con otro que es prioritario.

			Lo que busca esta meta es que se analicen los conflictos que hay en los requisitos, si hay conflictos realizar planes de mitigación a los conflictos, y esto hacerlo a nivel de los activos, en este caso software. La definición de funcionalidad junto con el análisis de requisitos a nivel de activos nos puede dar una idea de los conflictos, y con base a esto se pueden hacer los ajustes necesarios y desarrollar los planes de mitigación para resolver los conflictos. Estas definiciones ayudarán al entendimiento de cómo el software construido afectará los requisitos de resiliencia de empresa y de otros activos, entre ellos otras aplicaciones de la organización.
		RRD:SG3.SP3	**Validar Requisitos de Resiliencia** Teniendo una consistencia en los requisitos de resiliencia a nivel de activo, podemos decir que cumple con las expectativas de protección y sostenimiento que se necesitan, y si se asegura a este nivel, tendremos resiliencia en los servicios y en la operación de la organización. Con lo que proporciona RISK, tenemos que asegurarnos que hay requisitos de protección y sostenimiento tanto para el software como para su proceso de construcción. Del mismo modo, esta práctica busca optimizar los requisitos realizando una revisión en la que se detectarán los vacíos y con esto las actualizaciones o mejoras en los requisitos y en las medidas a implantar. De este modo, esta práctica proporciona un análisis entre objetivos estratégicos y requisitos de activos y un análisis de requisitos para asegurarse de qué se necesita para proteger y sostener el activo en relación con el servicio.
RMM	**RRM:SG1**	**RRM:SG1.SP1**	**Obtener un entendimiento de los Requisitos de Resiliencia** En el área de proceso RRD ya se establecen y definen los requisitos, de modo que ahora se deben entender, es decir que todos los propietarios de los servicios y los vigilantes y propietarios de los activos entiendan su rol y responsabilidad dentro de la implantación de la resiliencia en la organización. Para esto el área de proceso ADM tendrá un papel muy importante. Como se indicó anteriormente, en gran parte el propietario del activo tendrá que definir cuáles son los requisitos de resiliencia, en este caso el software. Esto lo hará basado en el entendimiento de la motivación de la organización y la búsqueda de la protección y sostenimiento del activo. Del mismo modo tendrá que tener en cuenta los requisitos de empresa y los análisis de la evaluación e impacto de los riesgos. Como producto de esta práctica tendremos los criterios de evaluación y aceptación de los requisitos por los vigilantes, y un acuerdo entre los propietarios y vigilantes del activo de mantener el conjunto de requisitos establecidos.
		RRM:SG1.SP2	**Obtener un compromiso con los Requisitos de Resiliencia** Es necesario que además de entender, haya un compromiso para la implementación de los requisitos establecidos. En esta práctica es significativo que la comunicación a los vigilantes, pues ellos estarán en contacto permanente y podrán entender lo que necesitan asegurar para el activo, por lo tanto se les debe comunicar lo que necesitan saber y que ellos hagan ese compromiso de implantar y mejorar los requisitos. Los propietarios serán los encargados de monitorizar y mejorar lo que suceda durante el ciclo de vida del activo. Como producto de esta práctica tenemos los compromisos documentados de requisitos y cambios en los requisitos, esto puede estar, por ejemplo en el acuerdo de nivel de servicio SLA.
		RRM:SG1.SP3	**Gestionar los cambios en los Requisitos de Resiliencia** La práctica anterior pide que se documente los compromisos en los cambios de los requisitos, esta práctica establece que haya un proceso definido de gestión para esos cambios. Es claro que las condiciones actuales de las organizaciones hacen que los escenarios de riesgo cambien y así mismo los requisitos de resiliencia, es por eso que se debe establecer este proceso que dicte los lineamientos para identificar y gestionar cambios. Se recomienda alinear la gestión del cambio con el marco que se implemente en la gestión de servicio de TI, bien sea ITIL o ISO 20000, y del mismo modo establecer los responsables y aprobadores de cambios. Como producto de esta práctica tendremos la base, el estatus, la base de datos –incluyendo historial de cambios, los criterios de cambio y peticiones de cambio de los requisitos.
		RRM:SG1.SP4	**Mantener la trazabilidad de los Requisitos de Resiliencia** Es importante seguir el ciclo de vida de los requisitos, su desarrollo, implementación y monitorización. La organización tiene que estar al tanto que las necesidades que tenía y que tradujo en requisitos, son satisfechas por las actividades propuestas. Es muy importante tener en cuenta el área de proceso RRD, pues teniendo claro los requisitos podemos realizar una matriz de trazabilidad y proponer un sistema para el seguimiento de los requisitos, con esto no solo conoceremos los activos que se relacionan sino con esto manejaremos los conflictos, y tendremos mucho más presente las

			interdependencias (Es claro que el software podrá soportar uno o más servicios de alto valor, o será parte de un grupo que soporte uno o más servicios)
		RRM:SG1.SP5	**Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos** Realizar la trazabilidad de la práctica anterior nos puede ayudar a la identificación y gestión de las inconsistencias entre requisitos y actividades, la idea es garantizar que se cumplen los compromisos con los requisitos y las actividades a desarrollar con el fin de garantizar la implementación de la resiliencia en la organización. En algunos casos a pesar de los esfuerzos, algunos requisitos no se cumplen porque dependen de más de un activo, en este caso se debe identificar y documentar esas inconsistencias para poder realizar las acciones correctivas pertinentes. Por esta razón se sugiere hacer revisiones de consistencia entre actividades y requisitos.
CTRL	**CTRL:SG1**	**CTRL:SG1.SP1**	**Definir los objetivos de control** Los objetivos de control son una manera de evaluar el rendimiento del sistema de control interno de la organización, sirve para garantizar un nivel apropiado de controles que le ayuden conseguir los objetivos estratégicos. Se pueden establecer objetivos de control, en TI por ejemplo, para asegurarse que el software y los sistemas consiguen los objetivos de una manera segura, eficaz y eficiente con un alto grado de protección y sostenimiento de un servicio de alto valor. Un ejemplo es el uso de objetivos de control es COBIT, para la gestión de TI. Pero así como definen algo general pueden llegar a definir algo específico. Es por esto que la definición es muy importante, pues para este caso de gestión de la resiliencia operacional, específicamente la resiliencia del software, los objetivos de control se definen en relación con los objetivos estratégicos de la organización, la información adquirida en RISK y en RRD. Los objetivos de control apuntarán a las estrategias de protección y sostenimiento de los activos relacionados con los servicios para asegurarse de que se gestiona su exposición a vulnerabilidades y amenazas. Con base en estos objetivos de control y las estrategias de protección y sostenimiento, se seleccionarán, analizarán y gestionarán los controles específicos. Como producto de esta práctica tendremos las directrices para la selección de los objetivos de control, los objetivos de control como tal, criterios para la priorización y lista de objetivos de control. Esto será importante a nivel general para establecer responsabilidades en la organización con base en los marcos de gestión como COBIT.
	CTRL:SG2	**CTRL:SG2.SP1**	**Definir los controles** Teniendo como referencia los objetivos de control y las estrategias de protección y sostenimiento de los servicios y activos de alto valor, se definirán los controles. Los controles no son necesariamente tecnológicos (Usando prácticas de *Secure Coding* nos ayuda a asegurar el producto, no necesariamente el proceso de implantación o entrega). Un control será una política, procedimiento, método, metodología, tecnología o herramienta que satisface un objetivo de control. Los controles que interesan a la gestión de resiliencia operacional son los que reducen la exposición a amenazas o vulnerabilidades que afectan a los activos y de este modo a los servicios y que ayudan a que esos mismos servicios y activos respondan y se recuperen mientras están en estado de interrupción. Estos controles podrán ser administrativos, técnicos o físicos a nivel general, y por su naturaleza preventivos (Separación de responsabilidades, documentación adecuada,…), detectivos (monitorización, auditorías,..), compensativos o correctivos. La práctica de esta parte es el listado de controles que protegen los servicios y activos. Controles a nivel de empresa, controles a nivel de servicio y activo y una matriz entre objetivos de control y controles (como la que ofrece COBIT). Del mismo modo asignar responsables para su implementación. Como estamos hablando específicamente de software, los controles específicos de producto son los que se implementen en el proceso TM.
	CTRL:SG3	**CTRL:SG3.SP1**	**Analizar los controles** Como una práctica ya conocida, es necesario realizar el análisis de los controles existentes, de modo que los controles concuerden con los requisitos de resiliencia y ayuden al logro de los objetivos de control. Adicionalmente es una oportunidad de considerar más controles, Como resultado de esta práctica encontramos el análisis de resultados, los objetivos que se satisfacen por los controles, vacíos en los controles, mejoras necesarias, controles propuestos, riesgos relacionados con objetivos de control no cubiertos y riesgos relacionados con riesgos redundantes y/o conflictivos
	CTRL:SG4	**CTRL:SG4.SP1**	**Evaluar los controles** Una vez hecho el análisis, es preciso evaluar si los controles satisfacen los requisitos de resiliencia establecidos. Esta es una manera de medir la efectividad de los controles de acuerdo a la iniciativa de resiliencia que tiene la organización. Esta evaluación debe hacerse de manera periódica, para poder mantener la gestión de los objetivos de control que estén orientados a la protección y sostenimiento de los servicios. El producto de esta práctica será la evaluación de los controles que contará con un alcance, unos resultados, áreas de problema, mejoras o actualizaciones a los controles existentes, nuevos controles propuestos, planes de remedio, actualizaciones a los planes de continuidad y riesgos relacionados a problemas sin resolver.

SC	**SC:SG1**	**SC:SG1.SP1**	**Planear la continuidad del servicio** En la tarea de proteger y sostener los activos, específicamente el sostenimiento dependerá de una estrategia efectiva de la continuidad del servicio. La organización debe enmarcar una estrategia de continuidad del negocio, y esta orientará la estrategia de la continuidad del servicio y su gestión para los procesos destinados a la planeación y ejecución de la sostenibilidad. LA idea es garantizar que los servicios de alto valor alcanzan la misión del servicio a pesar de situaciones de estrés y/o interrupción. Como primera medida se deberá elaborar el plan de continuidad del servicio para su desarrollo e implementación en los procesos de continuidad de servicio de la organización. La planeación mostrará el cómo la organización va a manejar la continuidad del servicio, y esto será una de las bases de la resiliencia operacional. El producto de esta práctica será el plan para la gestión de la continuidad del servicio –donde deberá estar alineado con: la posición de la organización frente a la continuidad del servicio; con la estructura del programa y los procesos de continuidad del servicio; con los requisitos relativos a la gestión de la resiliencia operacional del programa de continuidad del servicio; con los medios y las actividades relacionadas con la identificación y priorización de los servicios y activos para la continuidad; con las funciones y responsabilidades necesarias para llevar a cabo el plan y el programa; con las necesidades y requisitos de formación aplicables; con los recursos que serán necesarios para cumplir con los objetivos del plan; con los costos y presupuestos relevantes asociados a la continuidad del servicio. Y como es fundamental las peticiones de compromiso y el compromiso como tal que se haga con el plan deben estar documentados.
		SC:SG1.SP2	**Establecer estándares y directrices para la continuidad del servicio** Debido a la importancia de la continuidad del servicio, no se debe dejar de lado la implementación de mejores prácticas y aprender de los casos de éxito, por esto es necesario establecer y comunicar los estándares y directrices para la continuidad del servicio. Esto debe estar orientado a los objetivos de la organización. El producto serán las normas y directrices para la gestión de la continuidad del servicio. Estos serán desarrollados y comunicados resaltando responsabilidades, requisitos, entregas documentadas, modelo del contenido del plan, prueba de requisitos, y lo que se considere necesario para dejar claro el plan.
	SC:SG2	**SC:SG2.SP1**	**Identificar los servicios de alto valor para la organización** Para saber cuáles son los servicios a considerar, es necesario identificar y priorizar aquellos que son de alto valor, es decir aquellos que se requieren para que se cumpla la misión de la organización. Identificando estos servicios, será posible identificar el alcance y el tipo de plan de continuidad del servicio que se debe desarrollar e implementar. La idea es identificar los servicios de alto valor para la organización y sus activos asociados, esto puede basarse en lo que se defina en ADM En un marco de gestión de TI es claro que se tendrá claro cuáles son los objetivos de la empresa que se ven soportados por un servicio y que a su vez será un servicio de alto valor apoyado por un activo software. El resultado es la priorización de los servicios, actividades y activos asociados de alto valor (Apoyado por ADM). Igualmente los resultados de la evaluación de los riesgos en seguridad (Apoyado por RISK) y análisis de impacto en el negocio.
		SC:SG2.SP2	**Identificar dependencias e interdependencias internas y externas** Es claro que con el aumento de complejidad en las relaciones de las organizaciones, la resiliencia operacional cambia, por eso es importante para identificar y analizar las dependencias internas y externas y las interdependencias con el fin de asegurar la continuidad de servicio. En el caso de estudio deberá dejarse claras las responsabilidades de terceros sobre los servicios de la organización, manejar las relaciones y establecer responsabilidades. Como producto tendremos los proveedores de servicio de los cuales se depende, la lista de entidades externas que están incluidas en la entrega del servicio. El proceso ADM nos ayudará a identificar el activo que dependa de manera externa y la gestión con el área de proceso EXD.
		SC:SG2.SP3	**Identificar los registros y bases de datos organizacionales vitales** Una de los aspectos más importantes para la organización, y que está recogido en otra área de proceso CERT-RMM (*Knowledge and Information Management*) y que no tendremos en cuenta para esta guía es la resiliencia de la información. Para la organización la información es de vital importancia y mucho más si contribuye a los aspectos de la resiliencia operacional. Es por esto que se debe identificar la información vital requerida para la continuidad del servicio. Por lo tanto se deberán identificar y documentar los registros y bases de datos vitales, el personal fundamental y sus funciones específicas en el aprovisionamiento de los servicios, y asegurarse que los registros y bases de datos sean protegidos, accesibles y usables si ocurre una interrupción. A pesar que no concierne directamente a una medida a implementar en el software, si es una realidad que la información será importante en los sistemas resilientes.
	SC:SG3	**SC:SG3.SP1**	**Identificar los planes a ser desarrollados** Una vez establecido, se debe identificar cuáles son los planes de continuidad de servicio requeridos y que serán desarrollados, probados, ejecutados y mantenidos. Este

			deberá tenerse en cuenta durante el diseño e implementación de requisitos de resiliencia sobre los servicios y activos, es decir que para el software será importante que se tenga un trabajo paralelo en cuanto al plan y el soporte de los servicios o servicio al que vaya a soportar. Igualmente en este estará el resultado de las evaluaciones de riesgos en seguridad, las estimaciones del impacto, los requisitos de cumplimiento y considerando los Black Swan y las catástrofes.
		SC:SG3.SP2	**Desarrollar y documentar los planes de continuidad del servicio** Una vez identificados, se deben desarrollar y documentar los planes requeridos para la continuidad del servicio. Este se deberá realizar con base a los estándares y lineamientos establecidos. El software toma relevancia porque el personal de TI se involucra de manera significativa en el desarrollo y documentación del plan, en especial por los servicios que son automatizados o tienen una o más aplicaciones asociadas. Con el personal de TI y los propietarios del servicio en el equipo que elaborará los planes de continuidad, la resiliencia en el software será decisiva no solo por un servicio software directamente sino por otro tipo de servicios que puede soportar. Esta práctica nos dará como resultado las plantillas de los planes y los planes como tal para la continuidad del servicio. Dentro de esto deben recogerse los aspectos claves (p. ej. Actividades alternativas a desarrollar, recursos alternativos, activos de alto valor necesarios para soportar el plan), responsables e interesados.(Sobre todo si se implican terceros tener presente EXD), y cuestiones legales y de cumplimiento (p.ej. preparación frente a amenazas naturales o terrorismo)
		SC:SG3.SP3	**Asignar personal a los planes de continuidad del servicio** Para tener la certeza que el plan se ejecutará de manera eficaz, es necesario asignar miembros del personal a los planes de continuidad del servicio Al asignar personal, se deberá escoger personal que tenga las habilidades y responsabilidad de responder durante la ejecución del plan. Dependiendo del caso el personal será interno o externo (dependerá de contrato y SLA). Como producto de esta práctica tendremos los requisitos de personal a involucrar en el plan de continuidad del servicio, y la lista de miembros potenciales del personal. Una vez con esto queda asignar tareas al personal relacionado y establecer compromisos con las personas designadas. La organización se encargará también de la concienciación y formación del equipo.
		SC:SG3.SP4	**Almacenar y asegurar los planes de continuidad del servicio** Los planes de continuidad del servicio deben ser almacenados y accesibles a aquellos que lo necesiten, del mismo tienen que protegerse a través de controles de acceso que asegure que será accedido solo por aquel que sea autorizado
		SC:SG3.SP5	**Desarrollar el plan de formación para la continuidad del servicio** Para que un plan o una política tengan efecto en la organización hay que capacitar al personal, no solo del equipo sino general. Por lo tanto hay que desarrollar y administrar el entrenamiento en el plan de continuidad del servicio. Es importante que todos los involucrados en el plan tengan claras sus funciones y las responsabilidades que les competen. En algunos casos sirve para detectar vacíos de responsabilidad o habilidad en el personal. De esta práctica tendremos la lista de necesidades y vacíos del personal, una estrategia, unos materiales, unos registros y una retroalimentación de la evaluación de entrenamiento en el plan.
	SC:SG4	**SC:SG4.SP1**	**Validar los planes con requisitos y estándares** El fin de revisar el plan es que se satisfagan los requisitos y las necesidades de la organización en cuanto a resiliencia, por esta razón se tendrán que revisar los planes. Los planes de continuidad del servicio deben ser validados de modo que se eviten conflictos en el plan, que se compruebe que está alineado con lo que define la organización (estándares y directrices) y que se implementan los requisitos que establece RRD y RRM. Para esto se elabora una lista de requisitos que no se han cumplido, problemas de contenido y preocupaciones del plan, y un plan de actualizaciones y de medidas de remedio (los riesgos expuestos serán parte de RISK).
		SC:SG4.SP2	**Identificar y resolver los conflictos del plan** Debido a que hablamos de resiliencia operacional de la organización es normal que existan conflictos entre el mismo plan, debido a la cantidad de relaciones entre los activos, por esta razón se deberán identificar y resolver los conflictos, eso sí, bajo los parámetros de gestión del cambio que maneje la organización. En dado caso habrá que revisar o reescribir el plan.
	SC:SG5	**SC:SG5.SP1**	**Desarrollar programas y normas de pruebas** Lo que nos queda será probar el plan de continuidad del servicio, por lo tanto se deberá establecer e implementar un programa y unas normas para las pruebas. La organización deberá realizar estas pruebas en entornos controlados para asegurarse que el plan funciona y que cumple con su labor. Se debe establecer un programa,

			unas normas y unas fechas que permita saber que el software que soporta los servicios reaccionará ante las amenazas que se prevén en RISK y que se ven contempladas en RRD. Como resultado tendremos el programa y normas para los test considerando aspectos como estrategia de la organización, establecimiento de objetivos de calidad del test, nivel de involucre y compromiso de los interesados, reportes, revisión de aseguramiento de la calidad, directrices para manejar los problemas y directrices para la frecuencia
		SC:SG5.SP2	**Desarrollar y documentar planes de prueba** Una vez tenemos la referencia de los lineamientos, se desarrollaran y documentaran los planes de pruebas de continuidad del servicio. La importancia de documentar los procesos es que queda claro el guion, tanto lo que se quiere como los que participan, sus funciones, y los procedimientos. Se debe también tener en cuenta el entorno y tener muy claros los objetivos del test. Como resultado tendremos los planes para probar el plan de continuidad del servicio.
		SC:SG5.SP3	**Ejercer planes** Una vez teniendo la base, ahora tenemos que poner en marcha nuestras pruebas. Las pruebas nos arrojarán lo esperado en cuanto a eficacia, viabilidad y precisión a nivel general. Lo más importante serán los resultados de las pruebas, como forma de establecer que la organización está preparada para mantener el servicio estudiado, por eso deberán estar documentadas.
		SC:SG5.SP4	**Evaluar los resultados de las pruebas sobre el plan** Una vez hechos los test del plan de continuidad del servicio, revisaremos los resultados y los evaluaremos con el fin de encontrar mejoras y poder implantarlas. Lo esperado en estos casos es que los resultados del test sean los esperados de acuerdo a los objetivos definidos, y con la satisfacción del cumplimiento de los requisitos de entrada, pero no sucede así siempre. El producto de esta práctica serán el análisis documentado de los resultados, con los eventos no esperados y una lista de mejoras tanto al plan, y dependiendo de las circunstancias, al test.
	SC:SG6	**SC:SG6.SP1**	**Ejecutar planes** Una vez se definen los planes de continuidad del servicio y son probados, serán ejecutados y revisados. De manera inevitable los planes de continuidad del servicio se pondrán en marcha por diferentes razones. Lo que se espera es que se ejecuten como las condiciones lo requiere. Como buena práctica es que las condiciones se ejecuten en lo esperado y como lecciones aprendidas documentar la ejecución del plan.
		SC:SG6.SP2	**Medir la Efectividad del plan en operación** Después de la ejecución del plan, es necesario revisarlo post ejecución para identificar acciones correctivas que podrán ser implementadas como mejoras.
	SC:SG7	**SC:SG7.SP1**	**Establecer criterios de cambio** La ejecución real de los planes de continuidad del servicio nos dará condiciones reales en casos futuros, y aunque no es lo ideal, son lecciones aprendidas que serán aplicadas y que pueden mejorar y evitar consecuencias más graves. Por eso este proceso establece que los cambios a los planes de continuidad del servicio son identificados y gestionados. El producto de esta práctica son los criterios para hacer los cambios al plan de continuidad del servicio. Esto estará gestionado por los marcos de referencia que establezca la gestión de los cambios.
		SC:SG7.SP2	**Mantener los cambios a los planes** Al igual que se establecen los cambios, estos tienen que mantenerse bajo ciertas condiciones, y por los criterios que se establezcan. Por lo tanto de esta práctica se espera que sean las actualizaciones a los planes de continuidad y a la base de datos de los planes. Finalmente se buscará comunicar a la organización para que el personal esté al tanto de los cambios.
TM	**TM:SG1**	**TM:SG1.SP1**	**Priorizar los activos de tecnología** Hablar de software, para el Modelo CERT-RMM, es hablar de un activo de tipo tecnológico. La Gestión de TI que se establezca en la organización aportará en gran parte sobre todo a este proceso, teniendo en cuenta que manejará mejores prácticas para la gestión de activos de TI. Como se puede ver, la relación de las TI y los servicios pude llegar a ser significativa para la consecución de los objetivos que pone la compañía a nivel operacional. La priorización de estos activos tecnológicos es importante debido a que son recursos de gran importancia para la consecución de la misión de la organización por su soporte a la resiliencia operacional en cuanto a su contribución con los servicios. Toma importancia un activo, como el software, cuando se relaciona con activos de información, cuando lo provee un externo como servicio, si sirve para principios de redundancia, si aporta como control de la resiliencia de la organización o si hace parte de los planes que soportan la continuidad del servicio.

			Como resultado de esta práctica tenemos la lista de activos tecnológicos de alto valor (dentro del cual estará el software), que a su vez será suministrado por ADM y gestionado por nuestro marco de gestión de TI (Se sugiere COBIT), con esto podremos realizar de manera más eficaz la priorización y monitorización en caso de actualización
		TM:SG1.SP2	**Establecer los activos tecnológicos enfocados en la Resiliencia** Como se ha indicado, un software implementa resiliencia debido a la necesidad que tiene para la organización su funcionalidad en momentos de estrés o interrupción, pero esto quiere decir que posiblemente –y en su mayoría– soporta un servicio de alto valor para la organización –de los que estén en producción–, o ya sea que haga parte de los planes de restauración o ejecución de la continuidad del servicio. Esta práctica pretende que se identifiquen los activos de tecnología que soportan la continuidad del servicio y los planes de restauración. Con ayuda del marco de gestión de TI y el entorno de empresa que relaciona los servicios de alto valor, nos será fácil identificar los activos, y para nuestro caso el software que debe ser resiliente. Como producto de esta práctica tendremos la lista de los activos tecnológicos resilientes, y precisamente aquí se listará el software resiliente de la organización.
	TM:SG2	**TM:SG2.SP1**	**Asignar Requisitos de Resiliencia a los Activos de Tecnología** En esta práctica nos apoyaremos de lo definido en RRD, para establecer los requisitos de resiliencia a tener en cuenta por el activo, este será desde el punto de vista de gestión de la tecnología. ¿Por qué consideraremos en este paso estos requisitos?, esto es debido a que el software en sí mismo puede soportar o ser soportado por otro tipo de aplicaciones, con el fin de proteger y sostener el activo –una aplicación en sí misma puede protegerse con otra p. ej. Un sistema operativo puede necesitar de otra aplicación para su protección–. Es necesario identificar los conflictos de los requisitos y saberlos manejar. Finalmente tendremos documentados estos requisitos a tener en cuenta en el ciclo de vida del software que soporte los servicios
		TM:SG2.SP2	**Establecer e Implementar Controles** El sistema de control interno apoyará esta práctica, en cuanto a identificación e implementación de controles administrativos, técnicos y físicos que son requeridos para cumplir con los requisitos de resiliencia. Estos controles se implementarán con el fin de garantizar resiliencia operacional en los activos referentes a tecnología. Es claro que si se tiene una administración de la seguridad, como por ejemplo un SGSI basado en ISO 27001, y unos planes de continuidad, gran parte de los controles serán propuestos, pero los requisitos que nos proporcione RRD posiblemente nos harán implementar otros controles necesarios. Este punto es una motivación para establecer medidas dependiendo del tipo de software debido a que dentro de estos controles es importante establecerlos durante el diseño, construcción y adquisición como tal del software. Como producto de esta práctica tenemos identificados e implementaremos los controles administrativos (p. ej. Políticas a usuarios y de uso, Estándares de Interoperabilidad, procedimientos sobre personal…), técnicos (p. ej. Gestión del cambio y configuración, Aseguramiento de calidad de software, auditoría de software de grano fino,…) y físicos (aunque en el software será mucho más de soporte físico de operación) necesarios.
	TM:SG3	**TM:SG3.SP1**	**Identificar y evaluar los riesgos de activos de tecnología** Los activos tecnológicos estarán expuestos a riesgos, y el software igual, por esto se tendrá que identificar y evaluar los riesgos que le afectan. Esta práctica será conducida por los elementos que nos proporcione el marco de gestión de riesgos y las prácticas en RISK. Con esto podemos listar los riesgos que afectan a estos activos, en este caso el software (p.ej. riesgos de acciones intencionadas y no intencionadas que comprometen la protección, pobre implementación de controles que aseguren continuidad, pobre diseño y proceso de construcción…) y su impacto para la organización, esto se hará bajo criterios establecidos, de modo que con base a esto se establezca la categorización y priorización de los mismos.
		TM:SG3.SP2	**Mitigar los Riesgos Tecnológicos** Una vez identificados los riesgos a los que se ven comprometidos los activos de tecnología, es necesario establecer las medidas e implementarlas de acuerdo a la estrategia de la compañía. La idea es que el riesgo se encuentre en los niveles establecidos, y que se mitigue si se materializa a través de estrategias de protección que asegurarán el manejo del riesgo y la recuperación del activo sobre las consecuencias del impacto. Como resultado de esta práctica tendremos unos planes de mitigación junto a la lista de los responsables que van a conducir las estrategias de mitigación. Esto será monitorizado para posteriormente manejar el riesgo residual. De igual manera será soportado por el proceso RISK.
	TM:SG4	**TM:SG4.SP1**	**Controlar el acceso a los activos de tecnología** Para asegurarse que los activos de tecnología, y para nuestro caso el software, funcione de manera apropiada y con los resultados esperados es necesario gestionar su Integridad. El primer objetivo es asegurarse que el software no sea modificado, esto incluye la modificación no autorizada de código de software, sistemas, aplicaciones,

			sistemas operativos, herramientas y otros activos tecnológicos basados en software. La gestión de TI que implementa mejores prácticas, como COBIT –para la gestión de los activos de tecnología –, ISO 20000 o ITIL –para gestión de la configuración, gestión del cambio y gestión de la entrega–, e ISO 27001 –para controlar la seguridad (Triada CID)– podrán tener una ventaja competitiva para garantizar esto. El primer paso es controlar el acceso, esto quiere decir que existan medidas que controlen el acceso sólo a personal autorizado, y aseguren que no se hagan modificaciones conscientes e inconscientes del software. Estas medidas para el software suelen ser tecnológicas, a diferencia del hardware que implementa tanto medidas electrónicas como físicas. Hay que considerar los procedimientos que requerirán control de acceso, como modificaciones o actualizaciones, mantenimientos, conexiones a bases de datos, etc. Como producto de esta práctica tendremos que plantear políticas y procedimientos para el acceso (p.ej. Políticas para la gestión de acceso, Procesos de autorización de acceso, roles de usuario, políticas de gestión de identidades,…), implementar listas de control de acceso y herramientas necesarias de apoyo, así como una lista de miembros autorizados en la modificación del activo (relacionado con la gestión del cambio), en nuestro caso el software, logs y registros de auditoría.
		TM:SG4.SP2	**Ejecutar la gestión de la configuración** Uno de los aspectos contemplados dentro de la gestión de TI es la gestión de la configuración. Dentro de la resiliencia soporta la integridad de los activos de tecnología asegurando que pueden ser restaurados a un estado aceptable cuando sea necesario y provee un nivel de control sobre los cambios que afectan los servicios de la organización. La gestión de los servicios de TI establece los ítems de configuración, que son los elementos a gestionar, y para los cuales se realiza una gestión durante todo el ciclo de vida, desde sus fases de desarrollo, hasta su operación y mantenimiento, estableciendo controles durante su servicio. Se debe tener una atención especial con el software debido a que requieren estrictos niveles de control de la configuración, debido a la cantidad de cambios que se le realizan. El producto de esta práctica serán los procedimientos, políticas, directrices, normas y cuantos elementos crea la organización para gestionar la configuración de los activos de tecnología esto aplica tanto si el software es construido e implementado, usado o adquirido, tanto de manera interna como externa. Se sugiere el uso de ISO 20000 o ITIL, que implicará tenerlos en la Base de datos de configuración CMDB debidamente identificados y controlados –a través de logs y reportes–. Del mismo modo en esta práctica se propondrá las herramientas, técnicas y métodos que soportarán la gestión de la configuración. Esto a su vez podrá ser auditado. También se puede considerar unos planes de acción. Esta práctica será controlada por la gestión del cambio TM:SG4.SP3.
		TM:SG4.SP3	**Ejecutar la gestión y control del cambio** El software tiende a tener un comportamiento complejo debido a los modelos de madurez, los ciclos de desarrollo iterativos, requisitos emergentes, mejora de funcionalidades y demás, que lo hará estar en constante cambio durante su ciclo de vida, por lo tanto será trascendente que se gestionen los cambios. Los cambios tienen un papel importante en el software, por lo tanto tendrán que gestionarse para evaluar su impacto, ya sea económico, en el servicio que soporta, con otros activos que soporten servicios, etc. Del mismo modo, los cambios aportarán no solo a las mejoras, sino a la detección de fallos y mantenimiento, por eso una buena gestión garantiza un buen manejo alineado con los requisitos de la organización en cuanto a resiliencia. Como producto de esta práctica tenemos los puntos de referencia para suministrar a la gestión de configuración TM:SG4.SP2, pues la gestión del cambio se encarga de administrar los cambios a los elementos de configuración. Además establecerá las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para establecer los cambios, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, a las peticiones de cambio que se realicen se les debe hacer un respectivo seguimiento, el cual se almacenará en la base de datos de gestión del cambio.
		TM:SG4.SP4	**Ejecutar la gestión de la entrega** Para la gestión de servicios de TI, es necesario, del mismo modo como se establece la gestión de la configuración y del cambio, gestionar la entrega del activo tecnológico al entorno de producción. Para la gestión de la entrega en software es importante tener en cuenta el manejo de versiones, pero así mismo estas deben ser probadas antes de salir a producción y durante producción. En tecnología se maneja el término *Build* como una versión del activo que está listo para ser entregado en producción, en el caso del software puede ser por ejemplo una versión actualizada de un sistema de gestión que incorpora una mejora de seguridad. La entrega de los *builds* debe ser probada en un entorno para identificar situaciones que puedan comprometer otros activos, que refleje problemas de seguridad, etc. Una vez se identifique y se realicen las mejoras esperadas, de establecerá la entrega en producción. Así mismo en este proceso, los parches (que aportarán a la resiliencia en cuanto a mejorar el software en cuanto a gestión de vulnerabilidades) serán un tipo de entrega y tendrá que ser gestionado. Como producto de esta práctica se establecerán las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para la gestión de la entrega, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, se recomienda la entrega de *Builds*, pero del mismo modo se debe establecer un plan y procedimiento para probar las entregas, documentar los resultados de las pruebas a los *Builds*, establecer las mejoras y entregar a producción. La

			gestión de la entrega estará relacionada con los procesos de gestión de la configuración y del cambio.
	TM:SG5	TM:SG5.SP1	**Ejecutar la planeación para el sostenimiento de activos de tecnología** Así como se gestiona la integridad, para los activos de tecnología que soportan servicios, o que son de alto valor tienen que asegurar su disponibilidad y funcionalidad, por lo tanto deben desarrollarse planes que ayuden a su sostenimiento. Los requisitos de resiliencia establecidos, definirán ciertos términos en cuanto a disponibilidad que se deben cumplir, tanto en condiciones del día a día, como en el caso que se presente una situación de interrupción o estrés. Para esto se definen una serie de las métricas que permitan establecer la disponibilidad que debe cumplir la tecnología y servicios relacionados, tanto en condiciones normales como en condiciones degradadas. En este proceso, para cada activo se establece el *Recovery time objectives* (RTOs), que consiste en el periodo aceptable de baja de un activo tecnológico y su servicio asociado, después de que la organización se ve comprometida por una situación que impacta su operación normal, este será incluido en los planes de continuidad (Área de Proceso SC) debido a que está ligado al servicio. También se establece un *Recovery point objectives* (RPOs) en el cual se define el punto en el cuál un activo tecnológico debe ser restaurado para permitir la recuperación de los activos y servicios asociados después de la interrupción, este será incluido en los planes de continuidad (Área de Proceso SC) en cuanto a la restauración. Como producto de esta práctica se tendrá como referente los resultados del análisis de impacto en el negocio o la evaluación de riesgos (Área de Proceso RISK) con el fin de definir el alcance de sostenimiento de los activos. Igualmente se deben definir las métricas (Esto se definirá en RRD y RRM). También de recogerán los RTOs y los RPOs y esto se tendrá en cuenta en los planes de continuidad del servicio (Área de Proceso SC).
		TM:SG5.SP2	**Gestionar el mantenimiento de los activos de tecnología** Es claro que tendremos que establecer una práctica en la que se definan y se gestionen los mantenimientos operativos de los activos de tecnología. Tal vez esto suene mucho más para el hardware, sin embargo el ciclo de vida del software contempla el mantenimiento con el fin de mejorar el software, por ejemplo la aplicación de parches para corregir una vulnerabilidad u optimizar un algoritmo (gestionado por TM:SG4.SP4.). El riesgo de este tipo de mantenimiento, es una posible acción, intencionada o no, que podrá terminar comprometiendo los requisitos de resiliencia establecidos. Por esta razón, este tipo de mantenimiento necesita procedimientos de control, autorización y acceso. Como producto de esta práctica tenemos la lista de mantenimiento regular que requieren los activos de tecnología junto con intervalo y especificaciones, aunque en el caso del software consistiría en lo que se pacte de mantenimiento en la fase del ciclo de vida de desarrollo. Se deberá establecer una lista de personal autorizado para realizar las reparaciones. Se tendrá un documento de seguimiento con los mantenimientos registrados (tanto correctivo, preventivo, adaptativo o perfectivo). Se tendrán registradas las peticiones de mantenimiento. Esto deberá alinearse y estar controlado con la práctica que establece la gestión de cambios. En el caso de software es importante tener en cuenta la norma ISO/IEC 14764.
		TM:SG5.SP3	**Gestionar la capacidad de la tecnología** La gestión del servicio de TI, establece otra gestión que se debe hacer dentro de los activos de TI, y es la gestión de la capacidad. Para efectos de la guía, es importante tener en cuenta la capacidad operativa de los activos y poderla gestionar de manera adecuada esto debido a que la capacidad es una propiedad que está directamente relacionada a la disponibilidad. La planeación de la capacidad debe hacer previsiones, debido a la variabilidad que tiene la demanda del servicio (p.ej. horas pico y horas valle del servicio). En cuanto a software, la capacidad puede relacionarse con varias situaciones, por ejemplo usuarios concurrentes en una aplicación, la cantidad de peticiones que recibe, cantidad de espacio en memoria que utiliza, etc. El producto de esta práctica será el establecimiento de una estrategia que defina la gestión de la capacidad. Para construcción de software es importante que se defina en los requisitos de manera clara de la capacidad necesaria para el funcionamiento bajo cualquier condición. Adicionalmente se tendrá en cuenta marcos de referencia como ITIL e ISO 20000 para la gestión de la capacidad. Es recomendable hacer estimaciones y previsiones de las condiciones que cumplirá el software en cuanto a capacidad, por lo tanto es importante documentar los requisitos (previstos por RRD), y todos los procedimientos, políticas, planes, para su aseguramiento (esto puede afectar RPO y RTO). Para conocer el rendimiento de la estrategia, es importante establecer unas métricas para poder establecer planes de acción, y estos planes estarán ligados a los procesos de gestión de cambio.
		TM:SG5.SP4	**Gestionar la interoperabilidad de la tecnología** Actualmente la interoperabilidad de aplicaciones es un factor importante que se maneja en la organización, esto debido a las estructuras emergentes, virtualización e interconexión entre las empresas, y en general entre los sistemas. En el software específicamente se describe como la capacidad de diferentes aplicaciones de intercambiar los datos a través de formatos comunes, para entenderse en el mismo lenguaje. La importancia de gestionar la interoperabilidad es que es al día de hoy un importante factor que representa valor para la organización

			Como producto de esta práctica se establecerán los estándares seguidos para la interoperabilidad de modo que la arquitectura y diseño de la aplicación se basen en esos principios y mantengan el valor en cuanto a interoperabilidad minimizando los riesgos que esto implica (considerados por RISK). Se sugiere el uso de estándares para tener en cuenta en aspectos de diseño, desarrollo e implementación de arquitecturas interoperables, integración apropiada de sistemas (construidos, adquiridos o contratados), diseño adecuado de interfaces, manejo de "sistemas de sistemas", etc.
RTSE	**RTSE:SG1**	**RTSE:SG1.SP1**	**Identificar las directrices generales** El desarrollo de una solución técnica resiliente debe ser guiado por unas directrices que aseguren la consideración de actividades y controles durante todas las fases del ciclo de vida. Por esta razón se debe identificar de manera clara las directrices generales para aplicar la resiliencia en el software. La organización debe considerar en el proceso, metodología y ciclo de vida de desarrollo la integración de la seguridad y la continuidad del negocio, esto de acuerdo a los parámetros que establezcan los requisitos de resiliencia que plantea la organización y que garantizan que el software en sí será protegido y sostenible y hará resiliente los servicios que soporta. Las directrices deben comprender el entorno operacional de producción en el cuál se desarrollará el software, desarrollando análisis de compensación para hacer un balance entre requisitos y necesidades de resiliencia frente a costo y beneficios (p. ej. Analizar si vale la pena implementar el requisito de resiliencia si es más costoso que una interrupción en la operación). Adicionalmente es necesario tener en cuenta y hacer un análisis de los riesgos que implica en el ciclo de vida del proyecto la resiliencia frente a la continuidad de las operaciones para el servicio o servicios que el software soporta, junto a esto analizar las amenazas, y establecer medidas e hitos de progreso y cumplimiento. Como producto tendremos unos lineamientos generales para software y sistemas resilientes que se identificaran a través de: • Criterios de gestión de proyectos incluyendo o Definición de Objetivos del proyecto para resiliencia o Definición de Alcance de la resiliencia en el software o Entendimiento del entorno operativo y definición de restricciones del entorno donde será desplegado el software frente a la resiliencia. o Identificación de conceptos operacionales y escenarios asociados a la resiliencia o Análisis de compensación de necesidades y requisitos de resiliencia frente a costo y beneficio o Definición de criterios para aprobación de medidas resilientes durante el ciclo de vida del proyecto • Criterios de Gestión de Riesgos incluyendo o Identificación y análisis de los riesgos de resiliencia del proyecto (Provisionados por el área de proceso RISK) o Identificación y análisis de los riesgos de resiliencia del software durante todas las fases del ciclo de vida. • Análisis de Amenazas • Interconectividad e Interoperabilidad (Con base en TM:SG5.SP4.) • Identificación y priorización de controles incluyendo o Controles para proteger y sostener el servicio o los servicios que el software va a soportar. o Controles para proteger y sostener el software. o Controles para cadena de suministro del software, como cadena de custodia, privilegios de acceso, separación de responsabilidades, resistencia a cambios sin autorización (como códigos seguros y firmados) y evidencias de falsificación, protección persistente a información de alto valor, gestión del cumplimiento, inspección de código, testeo y verificación (Lo que se defina en CTRL) • Aseguramiento de la calidad, incluyendo métodos de validación y verificación deseados o logrados de la resiliencia de software • Medidas • Revisión y documentación necesaria para demostrar la finalización con éxito de cada fase del ciclo de vida. • Entrenamiento para Ingenieros de Software y Project managers Algunas iniciativas de NIST de ciclo de vida de desarrollo de software alineado con normas de seguridad de la información, SSE CMM (*Secure Software Engineering Capability Maturity Model*), BSIMM (*Building Security In Maturity Model*) y Microsoft SDLC pueden aportar gran base de conocimiento para esta práctica. Sin embargo

			una que tiene una amplia documentación y que está en auge sobre todo en desarrollo de aplicaciones web es OWASP (Anexo I), y en su proyecto SAMM encontramos un marco que es complementario y que se alinea con esta guía.
		RTSE:SG1.SP2	**Identificar las directrices de Requisitos** Así como se definen unas directrices generales, para los requisitos también se debe identificar unas directrices que permitan determinar los requisitos de resiliencia del software. Como bien es sabido la Ingeniería de Requisitos es vital para las soluciones software, sin embargo cuando hablamos de parámetros de calidad, seguridad y continuidad, estos no hacen parte habitual de las mejores prácticas a la hora de construir una solución. Siendo los requisitos la base del diseño del software, los requisitos de resiliencia del software deberán ser definidos desde el principio, garantizando así que se tienen en cuenta los lineamientos en cuanto a seguridad y continuidad de los servicios que vaya a soportar. El trabajo que implicará identificar estos requisitos, estará relacionado con el análisis de las necesidades que requiere cada servicio frente al software o sistema asociado. Deberá también tener en cuenta los requisitos de protección que ofrecerá con respecto a la confidencialidad, integridad y disponibilidad así como aprobación, no repudio, precisión, predictibilidad y confiabilidad. También es una buena práctica elaborar modelos de amenazas y escenarios en los cuales se comprometa la operación de un servicio de alto valor para saber si los requisitos cubren las necesidades y responden en un caso de estrés o interrupción. Como producto tendremos unos lineamientos de requisitos para software y sistemas resilientes que se identificaran a través de: • Obtención de requisitos de resiliencia (De los propietarios de los activos-servicios y de RRD Y RRM) • Análisis de riesgos durante la ingeniería de requisitos, el análisis será una entrada para definir la prioridad de los requisitos • Análisis de amenazas durante la ingeniería de requisitos • Análisis de compensación de requisitos (necesidades de propietarios del servicio, necesidades de stakeholders, consideraciones del ambiente operacional, etc.) • Conjeturas, decisiones y fundamentos • Métodos para representar perspectivas del defensor y el atacante, crear escenarios. (p. ej. contar con un equipo de profesionales de Hacking Ético, que se valgan de su experticia para aportar su conocimiento en cuanto a posibles vulnerabilidades y condiciones que pueden generar una condición anormal de operación. Esto generará muchos más requisitos que seguramente se obvian en el desarrollo normal de un proyecto software) • Control de Acceso • Gestión de Identidades • Seguridad de los Datos • Identificación y priorización de controles durante la ingeniería de requisitos (CTRL) • Análisis de cualquier software de tipo *open-source*, COTS(*Commercial off-the-shelf*) y *legacy* que sea parte del sistema, incluyendo la especificación de requisitos de resiliencia que tiene que cumplir cada software • Revisión de la especificación de los requisitos, incluyendo medidas para validad los niveles deseados o logrados de la resiliencia del software • Aseguramiento de la calidad durante la ingeniería de requisitos • Monitorizar y Auditar durante la ingeniería de requisitos • Mediciones durante la ingeniería de requisitos • Entrenamiento a los Ingenieros de Requisitos de Software Es importante considerar las prácticas de calidad que consideren en la organización para la ingeniería de requisitos, aunque se sugiere la norma ISO/IEC 9126-1:2001. *Software engineering -- Product quality* – y para la especificación de los requisitos la norma IEEE Std. 830-1998. IEEE *Recommended Practice for Software Requirements Specifications.*
		RTSE:SG1.SP3	**Identificar las directrices de Arquitectura y Diseño** El siguiente objetivo del ciclo de vida de desarrollo de software resiliente y una fase decisiva es la de la arquitectura y diseño. Esta práctica establece las directrices para diseñar resiliencia dentro del software y los sistemas.

			Una buena práctica en arquitectura y diseño hará que la implementación, montaje e integración del software se realice de manera óptima y que a nivel de resiliencia se haga sobre una base mucho más resiliente y resistente a interrupciones. Una especial atención en este proceso evitará dolores de cabeza a la hora de desarrollar cuando ya sea muy tarde implementar complementos para asegurar los requisitos establecidos. Una arquitectura y diseño resiliente basado en los requisitos definidos, protege y sostiene los servicios de acuerdo a los intereses de la organización, garantizando una respuesta adecuada a condiciones de interrupción y estrés. Las directrices de arquitectura y diseño para desarrollar software resiliente cubren los conceptos de diseño, arquitectura, diseño de componentes, diseño detallado y revisión y evaluación de diseño. Como producto tendremos unas directrices para el diseño y arquitectura de software y sistemas resilientes que se identificaran a través de: • Análisis de amenazas durante la arquitectura y diseño • Conjeturas, decisiones y fundamentos de diseño • *Attack Surface*, identificación de posibles alteraciones al software. • Métodos para representar perspectivas del defensor y el atacante, crear escenarios. • Patrones de diseño seguros a nivel de arquitectura y diseño • Control de Acceso • Gestión de Identidades • Seguridad de los Datos • Identificación y priorización de controles durante la arquitectura y diseño (CTRL) • Análisis de cualquier software de tipo open-source, COTS (*Commercial off-the-shelf*) y legacy, incluyendo la verificación de funcionalidades requeridas y comportamiento de resiliencia y ausencia de contenido malicioso. • Arquitecturas orientadas a servicios, virtualización y cloud computing (Software como Servicio) • Integración con arquitecturas existentes (Interconectividad e Interoperabilidad) • Análisis de riesgos durante la arquitectura y diseño • Análisis de la magnitud y complejidad del sistema, incluyendo los procesos de negocio de punta a punta y los análisis de fallos y vulnerabilidades del servicio • Inspecciones y revisiones de la arquitectura y el diseño, incluyendo validación de los niveles deseados o logrados de la resiliencia de software • Aseguramiento de la calidad durante la arquitectura y diseño • Monitorizar y Auditar durante la arquitectura y diseño • Mediciones durante la arquitectura y diseño • Entrenamiento a los arquitectos y diseñadores de software Para esto se sugiere apoyarse en la documentación de OWASP y la iniciativa SAMM de OWASP.
		RTSE:SG1.SP4	**Identificar las directrices de Implementación** La siguiente fase es la implementación, en la que se espera que se asegure que la resiliencia sea parte del ciclo de vida de codificación y pruebas del software. La idea es que se implementen todos los requisitos de resiliencia establecidos, como se ve reflejado en la arquitectura y diseño propuesto. Se debe trabajar bajo la premisa que un software resiliente es predecible en ejecución tanto en operación normal como en tiempo de estrés y que está libre de vulnerabilidades tanto como sea posible. Se deberán utilizar mejores prácticas tanto en la codificación como en las pruebas. Como producto tendremos unas directrices para la codificación de software resiliente, que a pesar de ser orientadas a proyecto se identificaran a través de: • Análisis de riesgos durante la codificación • Análisis de amenazas durante la codificación • Evaluación y Mitigación de *Attack Surface*. • Patrones de diseño seguros a nivel de implementación

			• Estándares de código seguro (Específicos del lenguaje)
			• Chequeos, inspecciones y revisiones del código y análisis estático y dinámico de código, incluyendo herramientas para soporte con el fin de verificar:
			  o Que se cumplen los requisitos de resiliencia
			  o Que se siguieron las directrices de arquitectura y diseño
			  o Ausencia de funciones prohibidas
			  o Ausencia de vulnerabilidades comúnmente conocidas
			  o Que se presenta el nivel deseado o logrado de resiliencia de software
			• Conducir revisiones más a fondo para los riesgos de mayor valor y códigos de mayor valor
			• Identificación y priorización de controles durante la codificación (CTRL)
			• Aseguramiento de la calidad durante la codificación
			• Monitorizar y Auditar durante la codificación
			• Mediciones durante la codificación
			• Entrenamiento a desarrolladores de software
			Además se deberán plantear unas directrices para la prueba de software resiliente, que a pesar de ser orientadas a proyecto se identificaran a través de
			• Análisis de riesgos durante las pruebas de software
			• Análisis de amenazas las pruebas de software
			• Reevaluación y Mitigación de *Attack Surface*.
			• A nivel de software, métodos para:
			  o Pruebas funcionales a requisitos de resiliencia
			  o Test de caja blanca, incluyendo análisis de cobertura de código
			  o Test de caja negra, que se enfoque en el comportamiento externo visible del software
			  o Fuzz testing
			  o Test de Penetración
			  o Test para vulnerabilidades específicas así como pruebas de regresión de vulnerabilidades
			  o Aplicación de modelos de amenaza y ataque
			  o Pruebas de software open-source, COTS y legacy, incluyendo la verificación de funcionalidades requeridas y comportamiento de resiliencia y ausencia de contenido malicioso
			  o Test de inspección en apoyo a la aprobación de entrega
			  o Test de regresión
			• Automatización de métodos y herramientas de prueba para apoyar la automatización
			• Revisiones de pruebas de software con el fin de verificar:
			  o Que se cumplen los requisitos de resiliencia
			  o Que se siguieron las directrices de arquitectura y diseño
			  o Ausencia de funciones prohibidas
			  o Ausencia de vulnerabilidades comúnmente conocidas
			  o Que se presenta el nivel deseado o logrado de resiliencia de software
			• Integridad y manejo de código (Incluyendo gestión de la configuración, cadena de custodia verificable, antifraude, monitoreo y análisis de eventos y logs de auditoría y firma de código)

			• Conducir revisiones más a fondo para los riesgos de mayor valor y códigos de mayor valor • Demostrar el cumplimiento con estándares de interoperabilidad (TM:SG5.SP4.) • Pruebas de controles durante las pruebas de software(CTRL) • Aseguramiento de la calidad durante las pruebas de software • Monitorizar y Auditar durante las pruebas de software • Mediciones durante las pruebas de software • Entrenamiento a Ingenieros de pruebas de software Para esto se sugiere apoyarse en la documentación de OWASP y la iniciativa SAMM de OWASP. Del mismo modo el uso de herramientas automatizadas que ya existen en el mercado para validación de códigos frente a vulnerabilidades.
		RTSE:SG1.SP5	**Identificar las directrices de Montaje e Integración** El software puede estar ligado a un sistema específico, por lo tanto su montaje e integración del software resiliente en sistemas resilientes tiene que definirse e identificarse. Para mantener la resiliencia del software, es necesario considerar que este será integrado a otros sistemas y que esto podrá afectar de manera significativa al entorno operacional de producción. Las vulnerabilidades pueden por varias razones, por tanto se deberán plantear las directrices que permitan hacer esto de la mejor manera. Tienen que ajustarse las formas de montaje e integración a las necesidades de negocio, a las mismas arquitecturas y considerar los escenarios que pueden influir, pues la resiliencia no es robusta si no se elabora una estrategia que permita mantener lo hecho en fases anteriores. El producto de esta práctica serán las directrices para el montaje e integración de las soluciones resilientes.
	RTSE:SG2	**RTSE:SG2.SP1**	**Seleccionar y ajustar directrices** Hay diversos tipos de software, e inclusive dentro de la misma organización alguno tendrá una función vital mientras otro puede rescindir de requisitos de resiliencia. Algunos necesitarán especial cuidado y requisitos específicos, en general dentro de la organización es un hecho que las directrices no aplicarán de manera estricta e igual a todo el software de la organización. Esta práctica dicta que se determinen las directrices para el proyecto de desarrollo de un software específico usando criterios de selección establecidos por la organización. Se tendrá en cuenta no solo el soporte a los servicios sino lo que nos ofrezca el área de proceso RRD. Una vez establecido el criterio se utilizará para seleccionar y ajustar las directrices de resiliencia para cada fase de ciclo de vida del proyecto software (RTSE:SG1). El producto de esta práctica serán los criterios de selección, las directrices de requisitos, arquitectura y diseño, implementación y montaje seleccionados. Se sugiere que los criterios de selección tengan en cuenta lo siguiente : • El valor de los servicios que el software planea soportar • El valor relativo del software de servicios que planea soportar • El grado en el cual el software maneja las acciones pedidas en los planes de mitigación de riesgo del servicio (junto con el correspondiente impacto y valoración del riesgo) • La prioridad de los requisitos y objetivos de resiliencia que deben ser satisfechos por el software • El análisis de compensación costo/beneficio, como la importancia relativa de identificar los defectos del software de manera temprana en el ciclo de vida del software frente al costo de implementar las directrices • Hacer análisis de compensación de la compra • La disponibilidad de personal debidamente capacitado • Los costos de capacitación del personal
		RTSE:SG2.SP2	**Integrar las directrices seleccionadas con un proceso definido de desarrollo de software y sistemas** Con las directrices definidas para cada fase del ciclo de vida, y seleccionadas para el software, ahora lo integraremos a un proceso definido de desarrollo de software y a un plan documentado.

			Las organizaciones que realizan la construcción de software, por lo general reúnen modelos y metodologías con el fin de definir, gestionar y mejorar un proceso para el desarrollo de aplicaciones. Muchas veces estas metodologías integran mejores prácticas de desarrollo y estimulan los procedimientos de calidad, pero dejan de lado consideraciones como la seguridad y la continuidad, es decir, dejan de lado la resiliencia. La consideración de esta práctica es integrar los procesos que establece la organización con las directrices seleccionadas, de modo que los sistemas cuenten con mejores prácticas de desarrollo, cumplan a cabalidad los requisitos funcionales, cuenten con propiedades de calidad, pero que también integren características de resiliencia definidas por la organización para interés de los servicios que se vayan a soportar. La idea es que el plan para un proyecto de desarrollo de un software específico se mejore y actualice con los requisitos y las directrices de resiliencia en las siguientes áreas: • Definición de los procesos de desarrollo • Tareas, medidas de progreso, hitos, entregables y la asignación de recursos (staff, capital, equipo, etc.) para implementar las directrices de resiliencia • Nuevos riesgos introducidos por las directrices de resiliencia y la elevación a una mayor prioridad de los riesgos actualmente identificados • Participación de los Stakeholder • Compromiso con el plan actualizado • Los criterios y autoridad de decisión en los principales hitos del proyecto Como producto de esta práctica tendremos las definiciones del proceso de desarrollo actualizado, igual que el plan de desarrollo.
	RTSE:SG3	**RTSE:SG3.SP1**	**Monitorear la ejecución del plan de desarrollo** El fin de esta práctica es asegurarse que se satisfacen los requisitos de resiliencia del software a través de la monitorización de la ejecución del plan de desarrollo. Debido a que el plan puede variar por diferentes condiciones, y que se pretende que en lo posible se mantenga la resiliencia, se monitorizará el proceso para asegurarse que el software satisface todos los requisitos definidos a un nivel apropiado de la fase del ciclo de vida. En caso que no se estén cumpliendo de manera satisfactoria los requisitos, los planes tendrán que ser actualizados y renegociados, y manejar el riesgo potencial y/o residual a través de RISK. La monitorización seguirá un proceso definido y estará ligada a la gestión de cambios establecida por la organización. Debería incluir coleccionar, analizar y reportar la efectividad de las directrices de resiliencia frente a cumplimiento, estado de los requisitos en cuanto a hitos planeados, identificación y planes de mitigación de riesgos, impactos a la continuidad del servicio para el software en desarrollo, impacto de los controles para proteger y sostener los servicios, software y sistemas, y mejoras a las directrices de resiliencia y definición de procesos que manejan la resiliencia. El producto de esta práctica será la definición de procedimientos para la revisión de los proyectos, medidas reportes y revisión de resultados del proyecto, actualización de los planes del proyecto, actualización de las directrices de resiliencia y de la definición de procesos.
		RTSE:SG3.SP2	**Entregar soluciones técnicas resilientes en producción** Una vez estamos seguros que el software cumple a cabalidad con los requisitos de resiliencia este puede ser entregado a producción, para esto tiene que comprobarse que se ha cumplido a satisfacción cada práctica anteriormente descrita. Antes de la entrega del activo software al entorno de producción operacional, estos activos deben ser sometidos a una inspección formal frente a los criterios documentados para asegurar que se han cumplido los requisitos de resistencia especificados. El resultado de los criterios de inspección satisfactorios es la aprobación para entregar el software a producción. Las prácticas sugeridas aquí son criterios, procedimientos y resultados de la inspección e implantación en entorno de producción con previo proceso de aprobación.

Tabla 17. Mapa de ruta para Software construido *in-house* basado en áreas de proceso CERT-RMM

5.1.2 Software Construido por externos

Área de Proceso	Metas	Prácticas	Recomendaciones
ADM	ADM:SG1	ADM:SG1.SP1	**Inventario de Activos** Es importante para la organización mantener de manera organizada sus activos, y del mismo modo se espera que la organización siga unas mejores prácticas en cuanto a la gestión de los mismos. Debido a que tratamos con software se debe tener en cuenta que al ser un activo intangible relacionado con tecnología, no tendrá un manejo igual al que tendrá un activo físico. De esta manera la gestión de TI debe asegure de establecer una adecuada gestión de activos de TI para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios, todo esto alineado con el marco de gobernanza de TI. En el caso del software construido por externos, se deberá tener claro en qué consiste el licenciamiento de producto, de quién es propiedad el software y demás términos que estarán incluidos en el contrato, pero aspectos que se refieran específicamente del software como producto. Un concepto importante es *Software Asset Management* (SAM), que corresponde a que a nivel de negocio se realice una adecuada gestión de la adquisición, mantenimiento, uso y disposición de las aplicaciones software dentro de la organización y la optimización de los procesos que se gestionan. Se sugiere utilizar marcos de gestión de software como ISO/IEC 19770 que se complementa con ISO 20000 en el proceso Gestión de la Configuración y en la cual la organización puede demostrar que realiza una gestión de activos de software. De igual manera ITILv3 incluye el proceso de Activos de Servicio y Gestión de la Configuración. COBIT 5 está alineado con ITILv3, por lo tanto puede considerar el inventario a alto nivel en la gestión de TI. Del mismo modo, SAM aporta a ISO/IEC 27002, en lo que a incidentes de seguridad de Software considera, es por esto que será un control preventivo a situaciones de interrupción o estrés. El producto de esta práctica debe ser un inventario y una base de datos del software de la organización. Del mismo modo se deberá identificar cuál software que se produce soporta procesos críticos del negocio y son vitales para la operación y la consecución de los objetivos de la organización. Se establecerá el valor de cada software que se produzca.
		ADM:SG1.SP2	**Establecer un Entendimiento Común** Es importante que se clasifiquen los activos software dentro de los activos de tecnología, del mismo modo, usando uno de los marcos sugeridos en ADM:SG1.SP1 se tendrá una buena práctica para que se manejen los activos de manera adecuada, y podrá ser el punto de partida para que se puedan asignar tanto a propietarios como vigilantes y entiendan sus responsabilidades (en la siguiente práctica ADM:SG1.SP3). El entendimiento será un punto de partida para evaluar las prioridades sobre los activos software en cuanto a resiliencia operacional, para saber cuáles tienen mayor valor para la organización en cuanto a resiliencia operacional no solo porque sean activos de alto valor sino también por los servicios que soporten, cuáles soportan servicios críticos y a partir de esto dará un enfoque global para establecer los requisitos de resiliencia. En este escenario, la organización encargada de la construcción de software será responsable de establecer las medidas necesarias para que su equipo sea consciente de lo que establece la organización contratante en cuanto a las responsabilidades y prioridades sobre los servicios. La organización contratante entregará a la organización contratada la documentación que considere necesaria para que se establezca de manera clara lo que requiere para su producto software y la organización contratada deberá asumir su responsabilidad sobre el proceso de construcción, por tanto también documentará el proceso. A través de esta práctica se llegará al entendimiento mutuo de los activos software y sobre todo cuáles son los de mayor importancia por soportar los servicios de la organización. Esto se puede realizar documentando la información necesaria, como políticas de uso, importancia y concienciación del activo frente a los servicios, entre otros.
		ADM:SG1.SP3	**Establecer Propietarios y Vigilantes** El software, como el resto de activos, tendrá asociados unos propietarios y unos vigilantes. Establecer mejores prácticas ADM:SG1.SP1 en general sobre los activos, y con un entendimiento común ADM:SG1.SP2 del aporte del software a la organización hará mucho más fácil establecer quién es quién dentro de las funciones del activo, y del mismo modo establecerá las pautas para la resiliencia operacional de la organización.

			Por un lado se establecerán los propietarios que tendrán la responsabilidad de la viabilidad, productividad y resiliencia del software, no necesariamente serán personas directamente, pueden ser unidades organizacionales internas o externas, esto debido a que dependerá de las definiciones que establezcan la organización contratada y la contratante. Por otro lado se establecerán vigilantes –que también serán personas o unidades organizacionales internas o externas– con la responsabilidad de implementar y gestionar los controles para satisfacer los requisitos de resiliencia, mientras estén a cargo del activo. Cabe resaltar que como se indicó anteriormente, en todos los casos, los propietarios son los responsables de asegurar la protección y continuidad apropiada de sus activos, sin tener en cuenta las acciones (o inacciones) de los vigilantes. El resultado de esta práctica será la identificación de los propietarios y los vigilantes y la actualización de los perfiles y las bases de datos de activos definidos. Es importante definir el perfil de propietario y vigilante y las responsabilidades que tienen con el software. En caso que el software soporte junto a un grupo de activos un servicio de la organización, es necesario establecer este grupo dentro de la identificación.
	ADM:SG2	**ADM:SG2.SP1**	**Asociar Activos con Servicios** Una práctica muy importante es empezar a establecer la relación de los activos con los servicios de la organización. Para una organización, asociar activos con los servicios es una práctica muy significativa debido a que es mucho más importante establecer resiliencia en un servicio de alto valor, que en un servicio complementario. La resiliencia operacional busca que la organización se enfoque en la visión de los servicios, debido a esto asociará el activo al servicio que soporta. En el caso del software, se tendrá clara no solo cuál será la funcionalidad y el para qué se construye, sino que se sabrá cuáles servicios van a asociarse y cuál será su rol para soportar el servicio. A partir de esta definición, será más fácil establecer las mejores estrategias en cuanto a protección y sostenimiento del software. Como resultado de esta práctica tendremos qué software se relaciona a los servicios de alto valor de la organización.
		ADM:SG2.SP2	**Analizar dependencias entre activos y servicios** Un activo puede soportar uno o más servicios, por esto se debe realizar un análisis general de estos servicios en la organización. Un CRM por ejemplo puede soportar varios servicios de la organización, y del funcionamiento de este podrán verse afectados uno o más servicios de alto valor. Una buena identificación de las dependencias es crucial pues será base para el establecimiento de los requisitos de resiliencia y por ende la estrategia de protección y sostenimiento del software. Como resultado de esta práctica evitaremos los conflictos potenciales por dependencias entre activos y se establecerán acciones y soluciones de mitigación.
	ADM:SG3	**ADM:SG3.SP1**	**Identificar Criterios de Cambios** (Esta práctica será complementaria a RRM:SG1.SP3) El ajuste a las necesidades de la organización y específicamente a los requisitos de resiliencia, afectará de manera directa al activo o a la asociación que tenga con un servicio, es por esto que se debe tener una práctica que sirva de soporte para el establecimiento y mantenimiento de los cambios. Los cambios identificados pueden afectar a uno o más activos, por esto las prácticas anteriores deberán soportar la estrategia de gestión del cambio establecida por la organización. Para este caso, la construcción del software por externos, aparte que la visión se enfocará en el proceso, por lo tanto habrán factores esenciales que tendrán que ser manejados y que podrían implicar cambios (requisitos nuevos, cambio de infraestructura y configuración, cambio de staff, caminos alternativos,…), se deberá tener en cuenta la dependencia de la relación contractual entre las partes. Los propietarios serán directamente capaces de establecer la aplicación y gestión de los cambios sobre el software. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
		ADM:SG3.SP2	**Mantener Cambios a los Activos e Inventarios** (Esta práctica será complementaria a RRM:SG1.SP3) Así como se identifican los cambios, es necesario gestionarlos de manera adecuada, teniendo en cuenta los marcos de referencia que utilice la organización para el mantenimiento de cambios. Hay diferentes condiciones que enfrentan a realizar cambios en el proceso de construcción de software, es importante acordar con la organización contratada una metodología para la gestión de los cambios, es decir, establecer en el contrato que la organización contratada cuente con mejores prácticas en la gestión de cambios y el tipo de cambios permitidos en el proceso. Esta práctica pretende que haya procedimientos documentados de la gestión de cambios en el activo y que se tenga presente el estado del activo en ciertos instantes, de acorde a esto establecer los requisitos de resiliencia y la estrategia de protección y sostenimiento del software y de los servicios que soportan.

			Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
EXD	**EXD:SG1**	**EXD:SG1.SP1**	**Identificar Dependencias externas** Este proceso es muy importante para este tipo de software. Cuando un tercero participa dentro de los procesos de la organización, la complejidad de las relaciones de la organización y los escenarios de riesgo aumentan. En este caso, construir, mantener o contratar software por un tercero. Estos terceros se considerarán dependencias externas, pues el activo –y el servicio– estará sujeto a las acciones de la entidad. Estas entidades tendrán que identificarse y priorizarse para asegurar la resiliencia de los servicios de alto valor que soportan, por lo tanto se identificará para entender, formalizar, monitorizar y gestionar los riesgos que esto ocasiona. Del mismo modo tener claro si soportan parte o todo un servicio y saber de qué activos son propietarios. Es importante recopilar toda la información, contratos entre proveedores, SLA, entre otros. El resultado de esta práctica será una lista detallada de las diferentes dependencias externas (descripción, activos y servicios que soportan, contratos,…), y un procedimiento documentado para la actualización de las mismas.
		EXD:SG1.SP2	**Priorizar dependencias externas** Es importante establecer prioridades sobre las entidades externas dependiendo de la importancia que tenga en la entrega de servicios de alto valor. Es importante realizar la priorización de dependencias externas pues la organización delega ciertas responsabilidades sobre los requisitos de resiliencia a dichas dependencias que manejan ciertos servicios, lo que le implica un papel importante para la consecución de la misión de la organización. El producto de esta práctica es establecer los criterios para priorizar estas entidades externas, y a partir de estos criterios se realizará la priorización de las dependencias externas, y los análisis de afinidad de las dependencias externas.
	EXD:SG2	**EXD:SG2.SP1**	**Identificar y evaluar riesgos debido a dependencias externas** Como se decía anteriormente, contratar una entidad externa aumenta la complejidad de las relaciones de la organización, pero también su entorno de riesgos. La gestión de riesgos de la organización juega un papel importante pues tiene que entender esa complejidad y ajustar la gestión a un número considerable de nuevos riesgos. Este proceso indica que se deben identificar y evaluar esos riesgos que se asumen al contratar a un tercero. Debido a que esto está involucrado en la gestión de riesgos se manejará en las prácticas RISK:SG3 y RISK:SG4. Por lo tanto el producto de esta práctica será las declaraciones de riesgos de dependencias externas con la evaluación de impacto y la lista de riesgos de las dependencias externas con categorización y priorización.
		EXD:SG2.SP2	**Mitigar riesgos debido a dependencias externas** La gestión de riesgos de la organización, entendiendo el nuevo escenario de riesgos que se crea, debe establecer e implementar las estrategias de mitigación, con el fin de mantener en un nivel aceptable de los riesgos derivados de las relaciones con dependencias externas. El producto de esta práctica serán los planes de mitigación de los riesgos de dependencias externas –donde se considera el desarrollo y revisión de controles– y la implementación y monitorización de la efectividad de los planes. Del mismo modo las prácticas serán complementadas por el proceso RISK:SG5.
	EXD:SG3	**EXD:SG3.SP1**	**Establecer especificaciones empresariales para dependencias externas** En general las relaciones con las entidades externas tienen que ser de tipo formal, a través de contratos o acuerdos que contribuyan seguridad al gobierno de la organización. Para escoger los proveedores, es necesario que estos demuestren que pueden cumplir lo que requiere la organización y que se ajustarán a las especificaciones del contrato. Al soportar servicios de la organización, las entidades externas se convierten en una extensión de la organización y la organización debe hacer que las entidades externas sean conscientes de la importancia de las políticas, estándares, lineamientos internos que a la larga son controles que ayudan a proteger y sostener las operación de la organización, siendo esto un apoyo para la resiliencia de la organización. Este pacto debe acordarse a nivel de empresa de modo que haya ese compromiso con la estrategia de resiliencia de la organización. Por esto a los externos se les compartirá los requisitos de resiliencia a nivel de empresa para que los tengan en cuenta RRD, y especificaciones referentes a los requisitos del software como tal (Por ejemplo, que el software se ajuste a los lineamientos establecidos por el Área de proceso RTSE, pues aunque no lo hace directamente se debe acordar que hayan prácticas como las ahí citadas).

			Como producto tendremos la lista de especificaciones de empresa que aplican a dependencias y entidades externas y las plantillas de acuerdo que reflejan las especificaciones empresariales.
		EXD:SG3.SP2	**Establecer especificaciones de resiliencia para dependencias externas** Así como a nivel de empresa se realiza este acuerdo, es necesario que se dejen claras las especificaciones de resiliencia que aplican para las entidades y dependencias externas. Una dependencia externa es el resultado del acceso de una entidad externa para controlar, desarrollar, poseer, ser responsable (de operación, mantenimiento o soporte), o tener obligaciones definidas relacionadas con uno o más activos o servicios de alto valor para la organización. Esos servicios tendrán unos requisitos de resiliencia y por ende la entidad externa tendrá un compromiso con el alcance de esos requisitos. Como producto de esta práctica se tendrán las especificaciones de resiliencia documentada y el acuerdo de nivel de servicio SLA. Es importante establecer comportamientos requeridos y normas de rendimiento esperados (disponibilidad, rendimiento, gestión del cambio, seguridad, continuidad del negocio…) con el fin de medir que se cumpla con los requisitos específicos.
		EXD:SG3.SP3	**Evaluar y seleccionar entidades externas** Como se ha indicado, el proceso de elección de un tercero para realizar un proceso como en este caso construir/mantener/implantar/ofrecer software, debe ser estricto y tener como referencia unas especificaciones claves y unos criterios de selección adecuados. Las entidades externas son seleccionadas basadas en una evaluación de su habilidad de cumplir con las especificaciones establecidas en EXD:SG3.SP1 y EXD:SG3.SP2. Es decir, adicional al proceso de contrato, deberá tenerse en cuenta cumplir con las expectativas de resiliencia necesarias Como producto de estas prácticas se deberá establecer un proceso de selección que incluya los requisitos esperados (preferiblemente a través de documentos que comprueben la capacidad de cumplimiento), establecer criterios de selección, evaluar las propuestas frente a los criterios y tomar una decisión.
		EXD:SG3.SP4	**Formalizar relaciones** Una vez tomada la decisión, lo que queda es establecer y mantener un acuerdo formal con la organización que ofrece las mejores condiciones de servicio y que cumple con las expectativas de la organización. El acuerdo dependerá del servicio o producto que se contrate, dependerá de la relación entre las entidades, los niveles de integración. Como producto de esta práctica tendremos el acuerdo con la entidad externa. En este acuerdo deberán estar cuestiones documentales como términos, condiciones, especificaciones, entre otros, al igual que permisos, licencias y demás. Deberá incluir también los manejos de desarrollo del trabajo, especificaciones, estándares de desarrollo y prácticas a utilizar para mantener el servicio, seguridad, gestión de riesgos, estrategias de protección y sostenimiento de producto y proceso, … Y cuanta documentación y aclaración necesite estar documentada orientado a tener los términos del servicio claro.
	EXD:SG4	**EXD:SG4.SP1**	**Monitorear rendimiento de entidades externas** Para saber el rendimiento de la entidad externa la mejor manera es monitorizando su actividad y esto lo hará de acuerdo a las especificaciones establecidas, estas serán el resultado de EXD:SG3. Esto se hará de manera periódica para tener un registro y en ciertos casos tomar decisiones. Algunos criterios de medición serán los que se establezca en el acuerdo formal. En algunos casos, los cambios que se hagan y las decisiones también dependerá del ambiente cambiante de riesgos. Como producto de esta práctica tenemos los reportes de las entidades externas, las bases de datos de gestión de relaciones que nos muestra la información de la monitorización del rendimiento actual, y reportes de inspección de entregas de la entidad externa. La monitorización deberá ser un procedimiento conocido y con responsables.
		EXD:SG4.SP2	**Corregir rendimiento de entidades externas** Dependiendo de los resultados monitorización realizada, se llevarán a cabo acciones correctivas para apoyar el rendimiento de la entidad externa, esto es muy importante en un ciclo de mejora continua. Entre menos dependa de externos la continuidad de los servicios, mejor. Las acciones correctivas estarán en el acuerdo. Como productos de esta sección tenemos los reportes o documentación de acciones correctivas, estas se evalúan y se escogen las mejores acciones correctivas entre las alternativas propuestas, y se realiza una documentación con las acciones correctivas escogidas. Esto debe comunicarse a la entidad externa. Como es mejora continua vendrá la implementación, monitorización y actualización en caso que se requiera.
RISK	**RISK:SG1**	**RISK:SG1.SP1**	**Determinar las categorías y fuentes de Riesgo** Es necesario que se establezcan las fuentes de riesgo a las que se va a exponer el software, no solo como producto sino como proceso, y a partir de esto establecer las

			categorías y una taxonomía del riesgo operacional, que es el que implica directamente la operación habitual de los servicios. Identificar el riesgo es comprender a qué se enfrentará el software, y a pesar de no poder contar con todos los escenarios posibles ni blindar la operación a todas las amenazas, lo más importante es identificar lo más crítico y considerar los *Black Swan.* Hay que considerar las fuentes tanto internas como externas. La organización debe establecer un marco para la gestión de riesgos que tenga una visión holística del software, como se indicó en el Capítulo 2 seguir un estándar como ISO 31000 junto con mejores prácticas para el ciclo de vida del software (no solo del producto sino del proceso) nos ayudará a establecer lo que se espera de esta práctica, el riesgo operacional al que se expone el software, las categorías de riesgo y la taxonomía. Este marco de referencia será el apoyo para la definición de los requisitos de resiliencia.
		RISK:SG1.SP2	**Establecer una estrategia para la Gestión de Riesgo Operacional** La organización que cuenta con un marco para la gestión del riesgo empresarial ERM, generalmente cuenta con la base necesaria para establecer la gestión de riesgo operacional ORM. De acuerdo como decida la organización su estrategia a nivel ejecutivo, decidirá cuál será la estrategia a seguir para la ORM que cumpla con los objetivos del negocio. La estrategia que se establezca será la que defina el desarrollo de las actividades relacionadas con la ORM y la colección, coordinación y gestión de dichos riesgos al marco de procesos de ERM. Dentro de la estrategia se debe contar con que el software se construye por externos, la construcción y el mantenimiento del software será responsabilidad de terceros, por lo tanto aumentará la complejidad de los escenarios de riesgos y del mismo modo habrá una delegación de responsabilidades en la gestión de riesgos. La estrategia debe estar documentada y comunicada a todos los interesados internos y externos responsables de las actividades de ORM, de modo que se tenga el entendimiento y sirva de entrada para otros procesos –por ejemplo para definir los requisitos de resiliencia.
	RISK:SG2	**RISK:SG2.SP1**	**Definir los parámetros de Riesgo** Para evaluar la relevancia del riesgo operacional en la organización, es preciso establecer unos parámetros con los cuales se pueda medir, es decir, se tenga una fotografía del estado actual de la organización. Para esto se definirán unos umbrales de tolerancia de riesgo que reflejará el nivel de riesgo dispuesto a admitir y a enfrentar la organización. Este deberá considerar que el riesgo implicará el proceso y el producto. La organización deberá exigir a la organización contratada lo que necesite para establecer estos parámetros y tenerlo en cuenta en su marco de gestión. Con un marco de gestión de riesgos, es claro que se establecerán estas medidas, y que acorde a la estrategia y objetivos de la organización se dictarán los parámetros a los que quiere apuntar y con los que evaluará el riesgo operacional, y con los cuáles definirá los requisitos para la gestión de riesgos.
		RISK:SG2.SP2	**Establecer criterios de medida del riesgo** Así como se definen los parámetros, es necesario definir los criterios para medir el impacto del riesgo dentro de la organización. Estos criterios serán importantes para clasificar, evaluar y priorizar los riesgos operacionales. El producto de esta práctica es el conocimiento de las áreas de impacto –donde el riesgo material tiene consecuencias significativas e interruptivas– priorización de dichas áreas y un documento con los criterios de medida y evaluación y con la probabilidad de riesgos.
	RISK:SG3	**RISK:SG3.SP1**	**Identificar los Niveles de riesgo en los Activos** Antes de establecer resiliencia operacional sobre los activos, es preciso que se tenga claro que los activos y por ende servicios se pueden ver afectados por los riesgos operacionales, por lo tanto su identificación y mitigación es primordial. Acorde a las categorías y al nivel de riesgo definidos por la organización, se identificarán los riesgos que afecten a los activos. Eso sí, es claro que no se identificará la totalidad de riesgos, pero al menos los riesgos operacionales que afecten los servicios, estos deben ser identificados y gestionados a través de diferentes técnicas. De ahí la importancia de seguir uno de los marcos para la gestión de riesgos. Deberá considerarse los escenarios en los cuales la gestión sea por parte de la organización, y pactar en el contrato los escenarios en los que sea parte del tercero. Como producto de esta práctica, tendremos un conjunto de herramientas para la identificación del riesgo organizacional, y una lista de riesgos categorizados por activo.
		RISK:SG3.SP2	**Identificar los Niveles de riesgo en los Servicios** El objeto de establecer la resiliencia operacional, es garantizar que los servicios cumplan la misión, sin embargo estos servicios están expuestos a unos riesgos operacionales que son el resultado de una serie de riesgos sobre los activos de la organización. Por esta razón hay que evaluarse el impacto potencial de un riesgo sobre un activo, en este caso los riesgos sobre el producto software y el proceso de construcción y funcionamiento, y su impacto sobre la misión del servicio. De acuerdo a esto no solo se puede mitigar sino priorizar teniendo en cuenta los intereses de la organización.

			Se asume que la organización identificó de manera esencial los servicios de alto valor, y en el proceso ADM los activos asociados a estos servicios. Como resultado de esto podremos clasificar los riesgos por servicio y establecer contextos donde afecta el servicio y consecuencias de los riesgos sobre los servicios si se llegan a materializar.
	RISK:SG4	**RISK:SG4.SP1**	**Evaluar Riesgos** Teniendo como lineamiento las prácticas realizadas anteriormente para la medición del riesgo (tolerancia, criterios e impactos del riesgo), lo siguiente es evaluar el riesgo operacional y sus consecuencias. Los riesgos varían en cada caso y específicamente para el software tenemos que considerar los diversos escenarios a los cuales esté expuesto el proceso. Esta evaluación nos dará una idea de cómo manejaremos el impacto de los riesgos y cómo actuar en diversas circunstancias operativas. El producto de esta práctica será la evaluación con base a los lineamientos de la organización y darle un valor cualitativo para poder decidir cómo actuar, y cómo priorizarlos.
		RISK:SG4.SP2	**Categorizar y Priorizar Riesgos** Una vez evaluados, podemos categorizar los riesgos operacionales de modo que establezcamos las prioridades sobre las actuaciones que se vayan a realizar sobre los mismos. Las categorías dependerán de los intereses, pero hay diferentes maneras de categorizas, por fuentes, por nivel de riesgo, por taxonomía, etc. Es importante tener en cuenta los escenarios y no olvidar los *Black Swan*, que en muchos casos son causas drásticas de interrupción o estrés del servicio. La priorización será importante a la hora de establecer resiliencia. Como resultado de esta práctica tendremos los riesgos por categorías y con priorización, de acuerdo a los intereses de la organización.
		RISK:SG4.SP3	**Asignar disposición al Riesgo** Del mismo modo que la organización asume que hay entendimiento de los riesgos, puesto que de acuerdo a su postura se evalúa, tiene también que documentar y aprobar su posición frente a los escenarios de riesgo identificados. Las acciones que tome de acuerdo a los riesgos tendrán que ser el producto de la estrategia establecida en la gestión de riesgos. La organización puede tomar diferentes disposiciones, entre ellas evitar el riesgo, aceptar el riesgo, transferir el riesgo o mitigar y controlar. Como producto de esta práctica de deberá listar los riesgos y la disposición de la organización, y los riesgos priorizados para mitigar. La disposición al riesgo será documentada y debidamente aprobada por la organización (en especial con los riesgos que se aceptarán).
	RISK:SG5	**RISK:SG5.SP1**	**Desarrollar planes para la mitigación del riesgo** Es necesario que se desarrollen planes de mitigación, sobre todo cuando el riesgo, producto de la evaluación realizada, está sobre el umbral y es inaceptable de admitir, no se desea transferir, y evitar solo sea posible eliminando la actividad que lo genera. La mitigación del riesgo puede requerir actividades referentes a la protección y sostenimiento del activo, o en algunos casos implementación de controles. En algunos casos las actividades no son suficientes y se deberá considerar el riesgo residual. Como práctica resultante tendremos el plan de mitigación del riesgo, para todos los riesgos a los que se dispuso mitigar y controlar. En este plan debe estar claro cómo se reduce la amenaza o cómo se protege la vulnerabilidad, las acciones preventivas, los controles a implementar, los planes de continuidad del servicio y los responsables del mismo, el costo del plan, manejo del riesgo residual.
		RISK:SG5.SP2	**Implementar estrategias de Riesgo** La organización toma una posición frente a los riesgos, y se espera que las estrategias que establece en la gestión de riesgos se sigan durante el todo el proceso, es por esto que los planes y estrategias de mitigación de riesgos serán implementados y además monitorizados. Lo que se gana con este ciclo continuo es que en un entorno cambiante de riesgos, debido a las nuevas condiciones de complejidad que se ve en las organizaciones de hoy en día, se tenga claro que la estrategia esté bien dirigida y los riesgos bien identificados, y en caso de cambios se revise y se modifique. El producto de esta práctica será la documentación de la implementación del plan de mitigación, y una visión actualizada del estado de los riesgos de acuerdo a la efectividad de la mitigación frente a las condiciones actuales, a través de la monitorización y unas políticas de seguimiento.
	RISK:SG6	**RISK:SG6.SP1**	**Revisar y ajustar estrategias para proteger los activos y servicios** Una de las formas de gestionar el riesgo operacional es la protección de activos y servicios, por lo tanto los controles que se implementen con este fin deben ser evaluados constantemente y actualizados según se requiera con base en la información que proporcione el riesgo. Los controles serán el resultado del proceso de gestión de riesgo o de los requisitos de resiliencia, la experiencia de la organización es la que le dará la madurez de la

			definición de estos controles, mejorar los actuales e implementar los que necesite, así como la consideración de controles que podrán proteger los activos y servicios de situaciones de riesgo emergentes. El producto de esta práctica será la lista de controles a revisar, mejorar o desarrollar y un plan de revisión.
		RISK:SG6.SP2	**Revisar y ajustar estrategias para sostener los activos y servicios** La otra forma de gestionar el riesgo operacional es el sostenimiento de activos y servicios, por lo tanto las estrategias de continuidad del servicio serán fundamentales de acuerdo al análisis que se realice en caso que el riesgo se materialice. Para esto se plantean planes de continuidad del servicio. Basado en la información de riesgo y lo aprendido en el ciclo de vida del riesgo, se pueden identificar falencias en la definición de los planes a través de las revisiones y posteriormente proponer mejoras. La validación de los planes será una manera de saber su efectividad frente a riesgos o amenazas operacionales El producto de esta práctica será la lista de planes de continuidad del servicio a revisar, mejorar o desarrollar y un plan de revisión.
RDD	**RRD:SG1**	**RRD:SG1.SP1**	**Establecer Requisitos de Resiliencia Empresarial** La organización a nivel de empresa, debe definir los requisitos de resiliencia con base a lo que necesite, generalmente motivados por la estrategia o cuestiones de cumplimiento. Debido a que el software es un activo de tipo "tecnología", los requisitos que se tendrán en cuenta son los que están ligados a la integridad y disponibilidad, si hace parte de un grupo de activos podrá también considerarse la confidencialidad. Como producto de esta práctica tenemos la lista de requisitos de resiliencia que define la empresa, que son el producto de la estrategia, objetivos, leyes, reglas y políticas, y deben ser comunicados y entendidos por las partes
	RRD:SG2	**RRD:SG2.SP1**	**Establecer Requisitos de Resiliencia de Activos** Una vez teniendo conciencia de los requisitos de empresa con los que se verá afectado el software, se tendrá que tener en cuenta como tal los requisitos de resiliencia que conciernen directamente al software. Es claro que estos requisitos se definirán con base en los servicios de alto valor que desee proteger y sostener la organización y por ende al activo que lo soporte, que para este caso es el software. Por tanto en esta práctica se deberá hacer una lista de lo que se considera en la organización como servicio de alto valor, establecer las relaciones entre servicios, procesos de negocio y para este caso específico el software asociado, y la lista de requisitos de resiliencia por cada software de la organización que esté asociado con un servicio de alto valor. Ya que hablamos de software, es importante que se realice una buena práctica para la ingeniería de requisitos, de modo que el software que se construya con los lineamientos necesarios, del mismo modo, que el proceso de construcción también cuente con las garantías para mantener la resiliencia operacional de la organización. Teniendo ya asociados unos propietarios (proceso ADM) y con buena parte de la evaluación de riesgos (RISK), esta identificación tiene una entrada de información significativa
		RRD:SG2.SP2	**Asignar Requisitos de Resiliencia Empresarial a los Servicios** Los requisitos de resiliencia que afectan los servicios deberán ser asignados a los servicios. Aquí se establecerá la relación necesaria para identificar la colección de requisitos de resiliencia para los servicios, a través de la asociación entre misión de empresa-misión de servicio-activo asociado. El producto de esta práctica es asociada a la lista de RRD:SG1.SP1y RRD:SG1.SP2 y tendrá en cuenta los servicios relevantes junto con los requisitos de resiliencia específicos por servicio. Con esto se identifica y asignan los requisitos aplicables bajo la relación requisito empresa -requisito de servicio-requisito de activo. Esto será de gran ayuda para establecer la relación del activo software con los requisitos de los servicios y la estrategia de resiliencia operacional de la organización.
	RRD:SG3	**RRD:SG3.SP1**	**Establecer una definición de la funcionalidad requerida** La organización debe tener definidas las funcionalidades requeridas de un activo en el contexto del servicio, por lo tanto es tener clara la funcionalidad que el software va a proporcionarle al servicio de la organización y cómo se va a mantener el software a través del ciclo de vida. Realizar una monitorización de esto proporciona una entrada para el análisis y validación de los requisitos de resiliencia a nivel de activo. Esta hace parte de la descripción del activo que se hará en ADM y estará documentada.
		RRD:SG3.SP2	**Analizar Requisitos de Resiliencia**

			Es claro que los requisitos de resiliencia buscan proteger y sostener los servicios, sin embargo también es de resaltar que en una organización hay requisitos que dependen de otros requisitos, o que tal vez un requisito entre en conflicto con otro que es prioritario. Lo que busca esta meta es que se analicen los conflictos que hay en los requisitos, si hay conflictos realizar planes de mitigación a los conflictos, y esto hacerlo a nivel de los activos, en este caso software. La definición de funcionalidad junto con el análisis de requisitos a nivel de activos nos puede dar una idea de los conflictos, y con base a esto se pueden hacer los ajustes necesarios y desarrollar los planes de mitigación para resolver los conflictos. Estas definiciones ayudarán al entendimiento de cómo el software construido afectará los requisitos de resiliencia de empresa y de otros activos, entre ellos otras aplicaciones de la organización. Esto deberá dejarse claro en el documento de requisitos que realice la organización contratada.
		RRD:SG3.SP3	**Validar Requisitos de Resiliencia** Teniendo una consistencia en los requisitos de resiliencia a nivel de activo, podemos decir que cumple con las expectativas de protección y sostenimiento que se necesitan, y si se asegura a este nivel, tendremos resiliencia en los servicios y en la operación de la organización. Con lo que proporciona RISK, tenemos que asegurarnos que hay requisitos de protección y sostenimiento tanto para el software como para su proceso de construcción. Del mismo modo, esta práctica busca optimizar los requisitos realizando una revisión en la que se detectarán los vacíos y con esto las actualizaciones o mejoras en los requisitos y en las medidas a implantar. De este modo, esta práctica proporciona un análisis entre objetivos estratégicos y requisitos de activos y un análisis de requisitos para asegurarse de qué se necesita para proteger y sostener el activo en relación con el servicio.
RMM	**RRM:SG1**	**RRM:SG1.SP1**	**Obtener un entendimiento de los Requisitos de Resiliencia** En el área de proceso RRD ya se establecen y definen los requisitos, de modo que ahora se deben entender, es decir que todos los propietarios de los servicios y los vigilantes y propietarios de los activos entiendan su rol y responsabilidad dentro de la implantación de la resiliencia en la organización. Para esto el área de proceso ADM tendrá un papel muy importante. Como se indicó anteriormente, en gran parte el propietario del activo tendrá que definir cuáles son los requisitos de resiliencia, en este caso el software. Esto lo hará basado en el entendimiento de la motivación de la organización y la búsqueda de la protección y sostenimiento del activo. Del mismo modo tendrá que tener en cuenta los requisitos de empresa y los análisis de la evaluación e impacto de los riesgos. Como producto de esta práctica tendremos los criterios de evaluación y aceptación de los requisitos por los vigilantes, y un acuerdo entre los propietarios y vigilantes del activo de mantener el conjunto de requisitos establecidos.
		RRM:SG1.SP2	**Obtener un compromiso con los Requisitos de Resiliencia** Es necesario que además de entender, haya un compromiso para la implementación de los requisitos establecidos. En esta práctica es significativo que la comunicación a los vigilantes, pues ellos estarán en contacto permanente y podrán entender lo que necesitan asegurar para el activo, por lo tanto se les debe comunicar lo que necesitan saber y que ellos hagan ese compromiso de implantar y mejorar los requisitos. Los propietarios serán los encargados de monitorizar y mejorar lo que suceda durante el ciclo de vida del activo. Como producto de esta práctica tenemos los compromisos documentados de requisitos y cambios en los requisitos, esto puede estar, por ejemplo en el acuerdo de nivel de servicio SLA.
		RRM:SG1.SP3	**Gestionar los cambios en los Requisitos de Resiliencia** La práctica anterior pide que se documente los compromisos en los cambios de los requisitos, esta práctica establece que haya un proceso definido de gestión para esos cambios. Es claro que las condiciones actuales de las organizaciones hacen que los escenarios de riesgo cambien y así mismo los requisitos de resiliencia, es por eso que se debe establecer este proceso que dicte los lineamientos para identificar y gestionar cambios. Se recomienda alinear la gestión del cambio con el marco que se implemente en la gestión de servicio de TI, bien sea ITIL o ISO 20000, y del mismo modo establecer los responsables y aprobadores de cambios. Como producto de esta práctica tendremos la base, el estatus, la base de datos –incluyendo historial de cambios, los criterios de cambio y peticiones de cambio de los requisitos.
		RRM:SG1.SP4	**Mantener la trazabilidad de los Requisitos de Resiliencia** Es importante seguir el ciclo de vida de los requisitos, su desarrollo, implementación y monitorización. La organización tiene que estar al tanto que las necesidades que tenía y que tradujo en requisitos, son satisfechas por las actividades propuestas.

			Es muy importante tener en cuenta el área de proceso RRD, pues teniendo claro los requisitos podemos realizar una matriz de trazabilidad y proponer un sistema para el seguimiento de los requisitos, con esto no solo conoceremos los activos que se relacionan sino con esto manejaremos los conflictos, y tendremos mucho más presente las interdependencias (Es claro que el software podrá soportar uno o más servicios de alto valor, o será parte de un grupo que soporte uno o más servicios)
		RRM:SG1.SP5	**Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos** Realizar la trazabilidad de la práctica anterior nos puede ayudar a la identificación y gestión de las inconsistencias entre requisitos y actividades, la idea es garantizar que se cumplen los compromisos con los requisitos y las actividades a desarrollar con el fin de garantizar la implementación de la resiliencia en la organización. En algunos casos a pesar de los esfuerzos, algunos requisitos no se cumplen porque dependen de más de un activo, en este caso se debe identificar y documentar esas inconsistencias para poder realizar las acciones correctivas pertinentes. Por esta razón se sugiere hacer revisiones de consistencia entre actividades y requisitos.
CTRL	**CTRL:SG1**	**CTRL:SG1.SP1**	**Definir los objetivos de control** Los objetivos de control son una manera de evaluar el rendimiento del sistema de control interno de la organización, sirve para garantizar un nivel apropiado de controles que le ayuden conseguir los objetivos estratégicos. Se pueden establecer objetivos de control, en TI por ejemplo, para asegurarse que el software y los sistemas consiguen los objetivos de una manera segura, eficaz y eficiente con un alto grado de protección y sostenimiento de un servicio de alto valor. Un ejemplo es el uso de objetivos de control es COBIT, para la gestión de TI. Pero así como definen algo general pueden llegar a definir algo específico. Es por esto que la definición es muy importante, pues para este caso de gestión de la resiliencia operacional, específicamente la resiliencia del software, los objetivos de control se definen en relación con los objetivos estratégicos de la organización, la información adquirida en RISK y en RRD. Los objetivos de control apuntarán a las estrategias de protección y sostenimiento de los activos relacionados con los servicios para asegurarse de que se gestiona su exposición a vulnerabilidades y amenazas. Con base en estos objetivos de control y las estrategias de protección y sostenimiento, se seleccionarán, analizarán y gestionarán los controles específicos. Como producto de esta práctica tendremos las directrices para la selección de los objetivos de control, los objetivos de control como tal, criterios para la priorización y lista de objetivos de control. Esto será importante a nivel general para establecer responsabilidades en la organización con base en los marcos de gestión como COBIT.
	CTRL:SG2	**CTRL:SG2.SP1**	**Definir los controles** Teniendo como referencia los objetivos de control y las estrategias de protección y sostenimiento de los servicios y activos de alto valor, se definirán los controles. Los controles no son necesariamente tecnológicos (Usando prácticas de *Secure Coding* nos ayuda a asegurar el producto, no necesariamente el proceso de implantación o entrega). Un control será una política, procedimiento, método, metodología, tecnología o herramienta que satisface un objetivo de control. Los controles que interesan a la gestión de resiliencia operacional son los que reducen la exposición a amenazas o vulnerabilidades que afectan a los activos y de este modo a los servicios y que ayudan a que esos mismos servicios y activos respondan y se recuperen mientras están en estado de interrupción. Estos controles podrán ser administrativos, técnicos o físicos a nivel general, y por su naturaleza preventivos (Separación de responsabilidades, documentación adecuada,…), detectivos (monitorización, auditorías,..), compensativos o correctivos. La práctica de esta parte es el listado de controles que protegen los servicios y activos. Controles a nivel de empresa, controles a nivel de servicio y activo y una matriz entre objetivos de control y controles (como la que ofrece COBIT). Del mismo modo asignar responsables para su implementación. Como estamos hablando específicamente de software, los controles específicos de producto son los que se implementen en el proceso TM.
	CTRL:SG3	**CTRL:SG3.SP1**	**Analizar los controles** Como una práctica ya conocida, es necesario realizar el análisis de los controles existentes, de modo que los controles concuerden con los requisitos de resiliencia y ayuden al logro de los objetivos de control. Adicionalmente es una oportunidad de considerar más controles, Como resultado de esta práctica encontramos el análisis de resultados, los objetivos que se satisfacen por los controles, vacíos en los controles, mejoras necesarias, controles propuestos, riesgos relacionados con objetivos de control no cubiertos y riesgos relacionados con riesgos redundantes y/o conflictivos
	CTRL:SG4	**CTRL:SG4.SP1**	**Evaluar los controles** Una vez hecho el análisis, es preciso evaluar si los controles satisfacen los requisitos de resiliencia establecidos. Esta es una manera de medir la efectividad de los controles de acuerdo a la iniciativa de resiliencia que tiene la organización. Esta evaluación debe hacerse de manera periódica, para poder mantener la gestión de los objetivos de control que estén orientados a la protección y sostenimiento de los servicios.

			El producto de esta práctica será la evaluación de los controles que contará con un alcance, unos resultados, áreas de problema, mejoras o actualizaciones a los controles existentes, nuevos controles propuestos, planes de remedio, actualizaciones a los planes de continuidad y riesgos relacionados a problemas sin resolver.
SC	**SC:SG1**	**SC:SG1.SP1**	**Planear la continuidad del servicio** En la tarea de proteger y sostener los activos, específicamente el sostenimiento dependerá de una estrategia efectiva de la continuidad del servicio. La organización debe enmarcar una estrategia de continuidad del negocio, y esta orientará la estrategia de la continuidad del servicio y su gestión para los procesos destinados a la planeación y ejecución de la sostenibilidad. LA idea es garantizar que los servicios de alto valor alcanzan la misión del servicio a pesar de situaciones de estrés y/o interrupción. Como primera medida se deberá elaborar el plan de continuidad del servicio para su desarrollo e implementación en los procesos de continuidad de servicio de la organización. La planeación mostrará el cómo la organización va a manejar la continuidad del servicio, y esto será una de las bases de la resiliencia operacional. El producto de esta práctica será el plan para la gestión de la continuidad del servicio –donde deberá estar alineado con: la posición de la organización frente a la continuidad del servicio; con la estructura del programa y los procesos de continuidad del servicio; con los requisitos relativos a la gestión de la resiliencia operacional del programa de continuidad del servicio; con los medios y las actividades relacionadas con la identificación y priorización de los servicios y activos para la continuidad; con las funciones y responsabilidades necesarias para llevar a cabo el plan y el programa; con las necesidades y requisitos de formación aplicables; con los recursos que serán necesarios para cumplir con los objetivos del plan; con los costos y presupuestos relevantes asociados a la continuidad del servicio. Y como es fundamental las peticiones de compromiso y el compromiso como tal que se haga con el plan deben estar documentados.
		SC:SG1.SP2	**Establecer estándares y directrices para la continuidad del servicio** Debido a la importancia de la continuidad del servicio, no se debe dejar de lado la implementación de mejores prácticas y aprender de los casos de éxito, por esto es necesario establecer y comunicar los estándares y directrices para la continuidad del servicio. Esto debe estar orientado a los objetivos de la organización. El producto serán las normas y directrices para la gestión de la continuidad del servicio. Estos serán desarrollados y comunicados resaltando responsabilidades, requisitos, entregas documentadas, modelo del contenido del plan, prueba de requisitos, y lo que se considere necesario para dejar claro el plan.
	SC:SG2	**SC:SG2.SP1**	**Identificar los servicios de alto valor para la organización** Para saber cuáles son los servicios a considerar, es necesario identificar y priorizar aquellos que son de alto valor, es decir aquellos que se requieren para que se cumpla la misión de la organización. Identificando estos servicios, será posible identificar el alcance y el tipo de plan de continuidad del servicio que se debe desarrollar e implementar. La idea es identificar los servicios de alto valor para la organización y sus activos asociados, esto puede basarse en lo que se defina en ADM En un marco de gestión de TI es claro que se tendrá claro cuáles son los objetivos de la empresa que se ven soportados por un servicio y que a su vez será un servicio de alto valor apoyado por un activo software. El resultado es la priorización de los servicios, actividades y activos asociados de alto valor (Apoyado por ADM). Igualmente los resultados de la evaluación de los riesgos en seguridad (Apoyado por RISK) y análisis de impacto en el negocio.
		SC:SG2.SP2	**Identificar dependencias e interdependencias internas y externas** Es claro que con el aumento de complejidad en las relaciones de las organizaciones, la resiliencia operacional cambia, por eso es importante para identificar y analizar las dependencias internas y externas y las interdependencias con el fin de asegurar la continuidad de servicio. En el caso de estudio deberá dejarse claras las responsabilidades de terceros sobre los servicios de la organización, manejar las relaciones y establecer responsabilidades. Como producto tendremos los proveedores de servicio de los cuales se depende, la lista de entidades externas que están incluidas en la entrega del servicio. El proceso ADM nos ayudará a identificar el activo que dependa de manera externa y la gestión con el área de proceso EXD.
		SC:SG2.SP3	**Identificar los registros y bases de datos organizacionales vitales** Una de los aspectos más importantes para la organización, y que está recogido en otra área de proceso CERT-RMM (*Knowledge and Information Management*) y que no tendremos en cuenta para esta guía es la resiliencia de la información. Para la organización la información es de vital importancia y mucho más si contribuye a los aspectos de la resiliencia operacional. Es por esto que se debe identificar la información vital requerida para la continuidad del servicio. Por lo tanto se deberán identificar y documentar los registros y bases de datos vitales, el personal fundamental y sus funciones específicas en el aprovisionamiento de los servicios, y asegurarse que los registros y bases de datos sean protegidos, accesibles y usables si ocurre una interrupción. A pesar que no concierne directamente a una medida a implementar en el software, si es una realidad que la información será importante en los sistemas resilientes.

	SC:SG3	**SC:SG3.SP1**	**Identificar los planes a ser desarrollados** Una vez establecido, se debe identificar cuáles son los planes de continuidad de servicio requeridos y que serán desarrollados, probados, ejecutados y mantenidos. Este deberá tenerse en cuenta durante el diseño e implementación de requisitos de resiliencia sobre los servicios y activos, es decir que para el software será importante que se tenga un trabajo paralelo en cuanto al plan y el soporte de los servicios o servicio al que vaya a soportar. Igualmente en este estará el resultado de las evaluaciones de riesgos en seguridad, las estimaciones del impacto, los requisitos de cumplimiento y considerando los Black Swan y las catástrofes.
		SC:SG3.SP2	**Desarrollar y documentar los planes de continuidad del servicio** Una vez identificados, se deben desarrollar y documentar los planes requeridos para la continuidad del servicio. Este se deberá realizar con base a los estándares y lineamientos establecidos. El software toma relevancia porque el personal de TI se involucra de manera significativa en el desarrollo y documentación del plan, en especial por los servicios que son automatizados o tienen una o más aplicaciones asociadas. Con el personal de TI y los propietarios del servicio en el equipo que elaborará los planes de continuidad, la resiliencia en el software será decisiva no solo por un servicio software directamente sino por otro tipo de servicios que puede soportar. Esta práctica nos dará como resultado las plantillas de los planes y los planes como tal para la continuidad del servicio. Dentro de esto deben recogerse los aspectos claves (p. ej. Actividades alternativas a desarrollar, recursos alternativos, activos de alto valor necesarios para soportar el plan), responsables e interesados.(Sobre todo si se implican terceros tener presente EXD), y cuestiones legales y de cumplimiento (p.ej. preparación frente a amenazas naturales o terrorismo)
		SC:SG3.SP3	**Asignar personal a los planes de continuidad del servicio** Para tener la certeza que el plan se ejecutará de manera eficaz, es necesario asignar miembros del personal a los planes de continuidad del servicio Al asignar personal, se deberá escoger personal que tenga las habilidades y responsabilidad de responder durante la ejecución del plan. Dependiendo del caso el personal será interno o externo (dependerá de contrato y SLA). Como producto de esta práctica tendremos los requisitos de personal a involucrar en el plan de continuidad del servicio, y la lista de miembros potenciales del personal. Una vez con esto queda asignar tareas al personal relacionado y establecer compromisos con las personas designadas. La organización se encargará también de la concienciación y formación del equipo.
		SC:SG3.SP4	**Almacenar y asegurar los planes de continuidad del servicio** Los planes de continuidad del servicio deben ser almacenados y accesibles a aquellos que lo necesiten, del mismo tienen que protegerse a través de controles de acceso que asegure que será accedido solo por aquel que sea autorizado
		SC:SG3.SP5	**Desarrollar el plan de formación para la continuidad del servicio** Para que un plan o una política tengan efecto en la organización hay que capacitar al personal, no solo del equipo sino general. Por lo tanto hay que desarrollar y administrar el entrenamiento en el plan de continuidad del servicio. Es importante que todos los involucrados en el plan tengan claras sus funciones y las responsabilidades que les competen. En algunos casos sirve para detectar vacíos de responsabilidad o habilidad en el personal. De esta práctica tendremos la lista de necesidades y vacíos del personal, una estrategia, unos materiales, unos registros y una retroalimentación de la evaluación de entrenamiento en el plan.
	SC:SG4	**SC:SG4.SP1**	**Validar los planes con requisitos y estándares** El fin de revisar el plan es que se satisfagan los requisitos y las necesidades de la organización en cuanto a resiliencia, por esta razón se tendrán que revisar los planes. Los planes de continuidad del servicio deben ser validados de modo que se eviten conflictos en el plan, que se compruebe que está alineado con lo que define la organización (estándares y directrices) y que se implementan los requisitos que establece RRD y RRM. Para esto se elabora una lista de requisitos que no se han cumplido, problemas de contenido y preocupaciones del plan, y un plan de actualizaciones y de medidas de remedio (los riesgos expuestos serán parte de RISK).
		SC:SG4.SP2	**Identificar y resolver los conflictos del plan** Debido a que hablamos de resiliencia operacional de la organización es normal que existan conflictos entre el mismo plan, debido a la cantidad de relaciones entre los activos, por esta razón se deberán identificar y resolver los conflictos, eso sí, bajo los parámetros de gestión del cambio que maneje la organización. En dado caso habrá que revisar o reescribir el plan.
	SC:SG5	**SC:SG5.SP1**	**Desarrollar programas y normas de pruebas**

			Lo que nos queda será probar el plan de continuidad del servicio, por lo tanto se deberá establecer e implementar un programa y unas normas para las pruebas. La organización deberá realizar estas pruebas en entornos controlados para asegurarse que el plan funciona y que cumple con su labor. Se debe establecer un programa, unas normas y unas fechas que permita saber que el software que soporta los servicios reaccionará ante las amenazas que se prevén en RISK y que se ven contempladas en RRD. Como resultado tendremos el programa y normas para los test considerando aspectos como estrategia de la organización, establecimiento de objetivos de calidad del test, nivel de involucre y compromiso de los interesados, reportes, revisión de aseguramiento de la calidad, directrices para manejar los problemas y directrices para la frecuencia
		SC:SG5.SP2	**Desarrollar y documentar planes de prueba** Una vez tenemos la referencia de los lineamientos, se desarrollaran y documentaran los planes de pruebas de continuidad del servicio. La importancia de documentar los procesos es que queda claro el guion, tanto lo que se quiere como los que participan, sus funciones, y los procedimientos. Se debe también tener en cuenta el entorno y tener muy claros los objetivos del test. Como resultado tendremos los planes para probar el plan de continuidad del servicio.
		SC:SG5.SP3	**Ejercer planes** Una vez teniendo la base, ahora tenemos que poner en marcha nuestras pruebas. Las pruebas nos arrojarán lo esperado en cuanto a eficacia, viabilidad y precisión a nivel general. Lo más importante serán los resultados de las pruebas, como forma de establecer que la organización está preparada para mantener el servicio estudiado, por eso deberán estar documentadas.
		SC:SG5.SP4	**Evaluar los resultados de las pruebas sobre el plan** Una vez hechos los test del plan de continuidad del servicio, revisaremos los resultados y los evaluaremos con el fin de encontrar mejoras y poder implantarlas. Lo esperado en estos casos es que los resultados del test sean los esperados de acuerdo a los objetivos definidos, y con la satisfacción del cumplimiento de los requisitos de entrada, pero no sucede así siempre. El producto de esta práctica serán el análisis documentado de los resultados, con los eventos no esperados y una lista de mejoras tanto al plan, y dependiendo de las circunstancias, al test.
	SC:SG6	**SC:SG6.SP1**	**Ejecutar planes** Una vez se definen los planes de continuidad del servicio y son probados, serán ejecutados y revisados. De manera inevitable los planes de continuidad del servicio se pondrán en marcha por diferentes razones. Lo que se espera es que se ejecuten como las condiciones lo requiere. Como buena práctica es que las condiciones se ejecuten en lo esperado y como lecciones aprendidas documentar la ejecución del plan.
		SC:SG6.SP2	**Medir la Efectividad del plan en operación** Después de la ejecución del plan, es necesario revisarlo post ejecución para identificar acciones correctivas que podrán ser implementadas como mejoras.
	SC:SG7	**SC:SG7.SP1**	**Establecer criterios de cambio** La ejecución real de los planes de continuidad del servicio nos dará condiciones reales en casos futuros, y aunque no es lo ideal, son lecciones aprendidas que serán aplicadas y que pueden mejorar y evitar consecuencias más graves. Por eso este proceso establece que los cambios a los planes de continuidad del servicio son identificados y gestionados. El producto de esta práctica son los criterios para hacer los cambios al plan de continuidad del servicio. Esto estará gestionado por los marcos de referencia que establezca la gestión de los cambios.
		SC:SG7.SP2	**Mantener los cambios a los planes** Al igual que se establecen los cambios, estos tienen que mantenerse bajo ciertas condiciones, y por los criterios que se establezcan. Por lo tanto de esta práctica se espera que sean las actualizaciones a los planes de continuidad y a la base de datos de los planes. Finalmente se buscará comunicar a la organización para que el personal esté al tanto de los cambios.
TM	**TM:SG1**	**TM:SG1.SP1**	**Priorizar los activos de tecnología** Hablar de software, para el Modelo CERT-RMM, es hablar de un activo de tipo tecnológico. La Gestión de TI que se establezca en la organización aportará en gran parte sobre todo a este proceso, teniendo en cuenta que manejará mejores prácticas para la gestión de activos de TI. Como se puede ver, la relación de las TI y los servicios pude llegar a ser significativa para la consecución de los objetivos que pone la compañía a nivel operacional. La priorización de estos activos tecnológicos es importante debido a que son recursos de gran importancia para la consecución de la misión de la organización por su soporte a la resiliencia operacional en cuanto a su

			contribución con los servicios. Toma importancia un activo, como el software, cuando se relaciona con activos de información, cuando lo provee un externo como servicio, si sirve para principios de redundancia, si aporta como control de la resiliencia de la organización o si hace parte de los planes que soportan la continuidad del servicio. Como resultado de esta práctica tenemos la lista de activos tecnológicos de alto valor (dentro del cual estará el software), que a su vez será suministrado por ADM y gestionado por nuestro marco de gestión de TI (Se sugiere COBIT), con esto podremos realizar de manera más eficaz la priorización y monitorización en caso de actualización
		TM:SG1.SP2	**Establecer los activos tecnológicos enfocados en la Resiliencia** Como se ha indicado, un software implementa resiliencia debido a la necesidad que tiene para la organización su funcionalidad en momentos de estrés o interrupción, pero esto quiere decir que posiblemente –y en su mayoría– soporta un servicio de alto valor para la organización –de los que estén en producción–, o ya sea que haga parte de los planes de restauración o ejecución de la continuidad del servicio. Esta práctica pretende que se identifiquen los activos de tecnología que soportan la continuidad del servicio y los planes de restauración. Con ayuda del marco de gestión de TI y el entorno de empresa que relaciona los servicios de alto valor, nos será fácil identificar los activos, y para nuestro caso el software que debe ser resiliente. Como producto de esta práctica tendremos la lista de los activos tecnológicos resilientes, y precisamente aquí se listará el software resiliente de la organización.
	TM:SG2	**TM:SG2.SP1**	**Asignar Requisitos de Resiliencia a los Activos de Tecnología** En esta práctica nos apoyaremos de lo definido en RRD, para establecer los requisitos de resiliencia a tener en cuenta por el activo, este será desde el punto de vista de gestión de la tecnología. ¿Por qué consideraremos en este paso estos requisitos?, esto es debido a que el software en sí mismo puede soportar o ser soportado por otro tipo de aplicaciones, con el fin de proteger y sostener el activo –una aplicación en sí misma puede protegerse con otra p. ej. Un sistema operativo puede necesitar de otra aplicación para su protección–. Es necesario identificar los conflictos de los requisitos y saberlos manejar. Finalmente tendremos documentados estos requisitos a tener en cuenta en el ciclo de vida del software que soporte los servicios
		TM:SG2.SP2	**Establecer e Implementar Controles** El sistema de control interno apoyará esta práctica, en cuanto a identificación e implementación de controles administrativos, técnicos y físicos que son requeridos para cumplir con los requisitos de resiliencia. Estos controles se implementarán con el fin de garantizar resiliencia operacional en los activos referentes a tecnología. Es claro que si se tiene una administración de la seguridad, como por ejemplo un SGSI basado en ISO 27001, y unos planes de continuidad, gran parte de los controles serán propuestos, pero los requisitos que nos proporcione RRD posiblemente nos harán implementar otros controles necesarios. Este punto es una motivación para establecer medidas dependiendo del tipo de software debido a que dentro de estos controles es importante establecerlos durante el diseño, construcción y adquisición como tal del software. Como producto de esta práctica tenemos identificados e implementaremos los controles administrativos (p. ej. Políticas a usuarios y de uso, Estándares de Interoperabilidad, procedimientos sobre personal…), técnicos (p. ej. Gestión del cambio y configuración, Aseguramiento de calidad de software, auditoría de software de grano fino,…) y físicos (aunque en el software será mucho más de soporte físico de operación) necesarios.
	TM:SG3	**TM:SG3.SP1**	**Identificar y evaluar los riesgos de activos de tecnología** Los activos tecnológicos estarán expuestos a riesgos, y el software igual, por esto se tendrá que identificar y evaluar los riesgos que le afectan. Esta práctica será conducida por los elementos que nos proporcione el marco de gestión de riesgos y las prácticas en RISK. Con esto podemos listar los riesgos que afectan a estos activos, en este caso el software (p.ej. riesgos de acciones intencionadas y no intencionadas que comprometen la protección, pobre implementación de controles que aseguren continuidad, pobre diseño y proceso de construcción…) y su impacto para la organización, esto se hará bajo criterios establecidos, de modo que con base a esto se establezca la categorización y priorización de los mismos.
		TM:SG3.SP2	**Mitigar los Riesgos Tecnológicos** Una vez identificados los riesgos a los que se ven comprometidos los activos de tecnología, es necesario establecer las medidas e implementarlas de acuerdo a la estrategia de la compañía. La idea es que el riesgo se encuentre en los niveles establecidos, y que se mitigue si se materializa a través de estrategias de protección que asegurarán el manejo del riesgo y la recuperación del activo sobre las consecuencias del impacto. Como resultado de esta práctica tendremos unos planes de mitigación junto a la lista de los responsables que van a conducir las estrategias de mitigación. Esto será monitorizado para posteriormente manejar el riesgo residual. De igual manera será soportado por el proceso RISK.

	TM:SG4	**TM:SG4.SP1**	**Controlar el acceso a los activos de tecnología** Para asegurarse que los activos de tecnología, y para nuestro caso el software, funcione de manera apropiada y con los resultados esperados es necesario gestionar su Integridad. El primer objetivo es asegurarse que el software no sea modificado, esto incluye la modificación no autorizada de código de software, sistemas, aplicaciones, sistemas operativos, herramientas y otros activos tecnológicos basados en software. La gestión de TI que implementa mejores prácticas, como COBIT –para la gestión de los activos de tecnología –, ISO 20000 o ITIL –para gestión de la configuración, gestión del cambio y gestión de la entrega–, e ISO 27001 –para controlar la seguridad (Triada CID)– podrán tener una ventaja competitiva para garantizar esto. El primer paso es controlar el acceso, esto quiere decir que existan medidas que controlen el acceso sólo a personal autorizado, y aseguren que no se hagan modificaciones conscientes e inconscientes del software. Estas medidas para el software suelen ser tecnológicas, a diferencia del hardware que implementa tanto medidas electrónicas como físicas. Hay que considerar los procedimientos que requerirán control de acceso, como modificaciones o actualizaciones, mantenimientos, conexiones a bases de datos, etc. Como producto de esta práctica tendremos que plantear políticas y procedimientos para el acceso (p.ej. Políticas para la gestión de acceso, Procesos de autorización de acceso, roles de usuario, políticas de gestión de identidades,…), implementar listas de control de acceso y herramientas necesarias de apoyo, así como una lista de miembros autorizados en la modificación del activo (relacionado con la gestión del cambio), en nuestro caso el software, logs y registros de auditoría.
		TM:SG4.SP2	**Ejecutar la gestión de la configuración** Uno de los aspectos contemplados dentro de la gestión de TI es la gestión de la configuración. Dentro de la resiliencia soporta la integridad de los activos de tecnología asegurando que pueden ser restaurados a un estado aceptable cuando sea necesario y provee un nivel de control sobre los cambios que afectan los servicios de la organización. La gestión de los servicios de TI establece los ítems de configuración, que son los elementos a gestionar, y para los cuales se realiza una gestión durante todo el ciclo de vida, desde sus fases de desarrollo, hasta su operación y mantenimiento, estableciendo controles durante su servicio. Se debe tener una atención especial con el software debido a que requieren estrictos niveles de control de la configuración, debido a la cantidad de cambios que se le realizan. El producto de esta práctica serán los procedimientos, políticas, directrices, normas y cuantos elementos crea la organización para gestionar la configuración de los activos de tecnología esto aplica tanto si el software es construido e implementado, usado o adquirido, tanto de manera interna como externa. Se sugiere el uso de ISO 20000 o ITIL, que implicará tenerlos en la Base de datos de configuración CMDB debidamente identificados y controlados –a través de logs y reportes–. Del mismo modo en esta práctica se propondrá las herramientas, técnicas y métodos que soportarán la gestión de la configuración. Esto a su vez podrá ser auditado. También se puede considerar unos planes de acción. Esta práctica será controlada por la gestión del cambio TM:SG4.SP3.
		TM:SG4.SP3	**Ejecutar la gestión y control del cambio** El software tiende a tener un comportamiento complejo debido a los modelos de madurez, los ciclos de desarrollo iterativos, requisitos emergentes, mejora de funcionalidades y demás, que lo hará estar en constante cambio durante su ciclo de vida, por lo tanto será trascendente que se gestionen los cambios. Los cambios tienen un papel importante en el software, por lo tanto tendrán que gestionarse para evaluar su impacto, ya sea económico, en el servicio que soporta, con otros activos que soporten servicios, etc. Del mismo modo, los cambios aportarán no solo a las mejoras, sino a la detección de fallos y mantenimiento, por eso una buena gestión garantiza un buen manejo alineado con los requisitos de la organización en cuanto a resiliencia. Como producto de esta práctica tenemos los puntos de referencia para suministrar a la gestión de configuración TM:SG4.SP2, pues la gestión del cambio se encarga de administrar los cambios a los elementos de configuración. Además establecerá las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para establecer los cambios, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, a las peticiones de cambio que se realicen se les debe hacer un respectivo seguimiento, el cual se almacenará en la base de datos de gestión del cambio.
		TM:SG4.SP4	**Ejecutar la gestión de la entrega** Para la gestión de servicios de TI, es necesario, del mismo modo como se establece la gestión de la configuración y del cambio, gestionar la entrega del activo tecnológico al entorno de producción. Para la gestión de la entrega en software es importante tener en cuenta el manejo de versiones, pero así mismo estas deben ser probadas antes de salir a producción y durante producción. En tecnología se maneja el término *Build* como una versión del activo que está listo para ser entregado en producción, en el caso del software puede ser por ejemplo una versión actualizada de un sistema de gestión que incorpora una mejora de seguridad. La entrega de los *builds* debe ser probada en un entorno para identificar situaciones que puedan comprometer otros activos, que refleje problemas de seguridad, etc. Una vez se identifique y se realicen las mejoras esperadas, de establecerá la entrega en producción. Así mismo en este proceso, los parches (que aportarán a la resiliencia en cuanto a mejorar el software en cuanto a gestión de vulnerabilidades) serán un tipo de entrega y tendrá que ser gestionado.

			Como producto de esta práctica se establecerán las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para la gestión de la entrega, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, se recomienda la entrega de *Builds*, pero del mismo modo se debe establecer un plan y procedimiento para probar las entregas, documentar los resultados de las pruebas a los *Builds*, establecer las mejoras y entregar a producción. La gestión de la entrega estará relacionada con los procesos de gestión de la configuración y del cambio.
	TM:SG5	**TM:SG5.SP1**	**Ejecutar la planeación para el sostenimiento de activos de tecnología** Así como se gestiona la integridad, para los activos de tecnología que soportan servicios, o que son de alto valor tienen que asegurar su disponibilidad y funcionalidad, por lo tanto deben desarrollarse planes que ayuden a su sostenimiento. Los requisitos de resiliencia establecidos, definirán ciertos términos en cuanto a disponibilidad que se deben cumplir, tanto en condiciones del día a día, como en el caso que se presente una situación de interrupción o estrés. Para esto se definen una serie de las métricas que permitan establecer la disponibilidad que debe cumplir la tecnología y servicios relacionados, tanto en condiciones normales como en condiciones degradadas. En este proceso, para cada activo se establece el *Recovery time objectives* (RTOs), que consiste en el periodo aceptable de baja de un activo tecnológico y su servicio asociado, después de que la organización se ve comprometida por una situación que impacta su operación normal, este será incluido en los planes de continuidad (Área de Proceso SC) debido a que está ligado al servicio. También se establece un *Recovery point objectives* (RPOs) en el cual se define el punto en el cuál un activo tecnológico debe ser restaurado para permitir la recuperación de los activos y servicios asociados después de la interrupción, este será incluido en los planes de continuidad (Área de Proceso SC) en cuanto a la restauración. Como producto de esta práctica se tendrá como referente los resultados del análisis de impacto en el negocio o la evaluación de riesgos (Área de Proceso RISK) con el fin de definir el alcance de sostenimiento de los activos. Igualmente se deben definir las métricas (Esto se definirá en RRD y RRM). También de recogerán los RTOs y los RPOs y esto se tendrá en cuenta en los planes de continuidad del servicio (Área de Proceso SC).
		TM:SG5.SP2	**Gestionar el mantenimiento de los activos de tecnología** Es claro que tendremos que establecer una práctica en la que se definan y se gestionen los mantenimientos operativos de los activos de tecnología. Tal vez esto suene mucho más para el hardware, sin embargo el ciclo de vida del software contempla el mantenimiento con el fin de mejorar el software, por ejemplo la aplicación de parches para corregir una vulnerabilidad u optimizar un algoritmo (gestionado por TM:SG4.SP4.). El riesgo de este tipo de mantenimiento, es una posible acción, intencionada o no, que podrá terminar comprometiendo los requisitos de resiliencia establecidos. Por esta razón, este tipo de mantenimiento necesita procedimientos de control, autorización y acceso. Como producto de esta práctica tenemos la lista de mantenimiento regular que requieren los activos de tecnología junto con intervalo y especificaciones, aunque en el caso del software consistiría en lo que se pacte de mantenimiento en la fase del ciclo de vida de desarrollo. Se deberá establecer una lista de personal autorizado para realizar las reparaciones. Se tendrá un documento de seguimiento con los mantenimientos registrados (tanto correctivo, preventivo, adaptativo o perfectivo). Se tendrán registradas las peticiones de mantenimiento. Esto deberá alinearse y estar controlado con la práctica que establece la gestión de cambios. En el caso de software es importante tener en cuenta la norma ISO/IEC 14764.
		TM:SG5.SP3	**Gestionar la capacidad de la tecnología** La gestión del servicio de TI, establece otra gestión que se debe hacer dentro de los activos de TI, y es la gestión de la capacidad. Para efectos de la guía, es importante tener en cuenta la capacidad operativa de los activos y poderla gestionar de manera adecuada esto debido a que la capacidad es una propiedad que está directamente relacionada a la disponibilidad. La planeación de la capacidad debe hacer previsiones, debido a la variabilidad que tiene la demanda del servicio (p.ej. horas pico y horas valle del servicio). En cuanto a software, la capacidad puede relacionarse con varias situaciones, por ejemplo usuarios concurrentes en una aplicación, la cantidad de peticiones que recibe, cantidad de espacio en memoria que utiliza, etc. El producto de esta práctica será el establecimiento de una estrategia que defina la gestión de la capacidad. Para construcción de software es importante que se defina en los requisitos de manera clara de la capacidad necesaria para el funcionamiento bajo cualquier condición. Adicionalmente se tendrá en cuenta marcos de referencia como ITIL e ISO 20000 para la gestión de la capacidad. Es recomendable hacer estimaciones y previsiones de las condiciones que cumplirá el software en cuanto a capacidad, por lo tanto es importante documentar los requisitos (previstos por RRD), y todos los procedimientos, políticas, planes, para su aseguramiento (esto puede afectar RPO y RTO). Para conocer el rendimiento de la estrategia, es importante establecer unas métricas para poder establecer planes de acción, y estos planes estarán ligados a los procesos de gestión de cambio.
		TM:SG5.SP4	**Gestionar la interoperabilidad de la tecnología** Actualmente la interoperabilidad de aplicaciones es un factor importante que se maneja en la organización, esto debido a las estructuras emergentes, virtualización e

			interconexión entre las empresas, y en general entre los sistemas. En el software específicamente se describe como la capacidad de diferentes aplicaciones de intercambiar los datos a través de formatos comunes, para entenderse en el mismo lenguaje. La importancia de gestionar la interoperabilidad es que es al día de hoy un importante factor que representa valor para la organización Como producto de esta práctica se establecerán los estándares seguidos para la interoperabilidad de modo que la arquitectura y diseño de la aplicación se basen en esos principios y mantengan el valor en cuanto a interoperabilidad minimizando los riesgos que esto implica (considerados por RISK). Se sugiere el uso de estándares para tener en cuenta en aspectos de diseño, desarrollo e implementación de arquitecturas interoperables, integración apropiada de sistemas (construidos, adquiridos o contratados), diseño adecuado de interfaces, manejo de "sistemas de sistemas", etc.
RTSE	**RTSE:SG1**	**RTSE:SG1.SP1**	**Identificar las directrices generales** El desarrollo de una solución técnica resiliente debe ser guiado por unas directrices que aseguren la consideración de actividades y controles durante todas las fases del ciclo de vida. Por esta razón se debe identificar de manera clara las directrices generales para aplicar la resiliencia en el software. La organización debe considerar en el proceso, metodología y ciclo de vida de desarrollo la integración de la seguridad y la continuidad del negocio, esto de acuerdo a los parámetros que establezcan los requisitos de resiliencia que plantea la organización y que garantizan que el software en sí será protegido y sostenible y hará resiliente los servicios que soporta. Las directrices deben comprender el entorno operacional de producción en el cuál se desarrollará el software, desarrollando análisis de compensación para hacer un balance entre requisitos y necesidades de resiliencia frente a costo y beneficios (p. ej. Analizar si vale la pena implementar el requisito de resiliencia si es más costoso que una interrupción en la operación). Adicionalmente es necesario tener en cuenta y hacer un análisis de los riesgos que implica en el ciclo de vida del proyecto la resiliencia frente a la continuidad de las operaciones para el servicio o servicios que el software soporta, junto a esto analizar las amenazas, y establecer medidas e hitos de progreso y cumplimiento. Como producto tendremos unos lineamientos generales para software y sistemas resilientes que se identificaran a través de: • Criterios de gestión de proyectos incluyendo o Definición de Objetivos del proyecto para resiliencia o Definición de Alcance de la resiliencia en el software o Entendimiento del entorno operativo y definición de restricciones del entorno donde será desplegado el software frente a la resiliencia. o Identificación de conceptos operacionales y escenarios asociados a la resiliencia o Análisis de compensación de necesidades y requisitos de resiliencia frente a costo y beneficio o Definición de criterios para aprobación de medidas resilientes durante el ciclo de vida del proyecto • Criterios de Gestión de Riesgos incluyendo o Identificación y análisis de los riesgos de resiliencia del proyecto (Provisionados por el área de proceso RISK) o Identificación y análisis de los riesgos de resiliencia del software durante todas las fases del ciclo de vida. • Análisis de Amenazas • Interconectividad e Interoperabilidad (Con base en TM:SG5.SP4.) • Identificación y priorización de controles incluyendo o Controles para proteger y sostener el servicio o los servicios que el software va a soportar. o Controles para proteger y sostener el software. o Controles para cadena de suministro del software, como cadena de custodia, privilegios de acceso, separación de responsabilidades, resistencia a cambios sin autorización (como códigos seguros y firmados) y evidencias de falsificación, protección persistente a información de alto valor, gestión del cumplimiento, inspección de código, testeo y verificación (Lo que se defina en CTRL) • Aseguramiento de la calidad, incluyendo métodos de validación y verificación deseados o logrados de la resiliencia de software • Medidas • Revisión y documentación necesaria para demostrar la finalización con éxito de cada fase del ciclo de vida.

			• Entrenamiento para Ingenieros de Software y Project managers Algunas iniciativas de NIST de ciclo de vida de desarrollo de software alineado con normas de seguridad de la información, SSE CMM (*Secure Software Engineering Capability Maturity Model*), BSIMM (*Building Security In Maturity Model*) y Microsoft SDLC pueden aportar gran base de conocimiento para esta práctica. Sin embargo una que tiene una amplia documentación y que está en auge sobre todo en desarrollo de aplicaciones web es OWASP (Anexo I), y en su proyecto SAMM encontramos un marco que es complementario y que se alinea con esta guía.
		RTSE:SG1.SP2	**Identificar las directrices de Requisitos** Así como se definen unas directrices generales, para los requisitos también se debe identificar unas directrices que permitan determinar los requisitos de resiliencia del software. Como bien es sabido la Ingeniería de Requisitos es vital para las soluciones software, sin embargo cuando hablamos de parámetros de calidad, seguridad y continuidad, estos no hacen parte habitual de las mejores prácticas a la hora de construir una solución. Siendo los requisitos la base del diseño del software, los requisitos de resiliencia del software deberán ser definidos desde el principio, garantizando así que se tienen en cuenta los lineamientos en cuanto a seguridad y continuidad de los servicios que vaya a soportar. El trabajo que implicará identificar estos requisitos, estará relacionado con el análisis de las necesidades que requiere cada servicio frente al software o sistema asociado. Deberá también tener en cuenta los requisitos de protección que ofrecerá con respecto a la confidencialidad, integridad y disponibilidad así como aprobación, no repudio, precisión, predictibilidad y confiabilidad. También es una buena práctica elaborar modelos de amenazas y escenarios en los cuales se comprometa la operación de un servicio de alto valor para saber si los requisitos cubren las necesidades y responden en un caso de estrés o interrupción. Como producto tendremos unos lineamientos de requisitos para software y sistemas resilientes que se identificaran a través de: • Obtención de requisitos de resiliencia (De los propietarios de los activos-servicios y de RRD Y RRM) • Análisis de riesgos durante la ingeniería de requisitos, el análisis será una entrada para definir la prioridad de los requisitos • Análisis de amenazas durante la ingeniería de requisitos • Análisis de compensación de requisitos (necesidades de propietarios del servicio, necesidades de stakeholders, consideraciones del ambiente operacional, etc.) • Conjeturas, decisiones y fundamentos • Métodos para representar perspectivas del defensor y el atacante, crear escenarios. (p. ej. contar con un equipo de profesionales de Hacking Ético, que se valgan de su experticia para aportar su conocimiento en cuanto a posibles vulnerabilidades y condiciones que pueden generar una condición anormal de operación. Esto generará muchos más requisitos que seguramente se obvian en el desarrollo normal de un proyecto software) • Control de Acceso • Gestión de Identidades • Seguridad de los Datos • Identificación y priorización de controles durante la ingeniería de requisitos (CTRL) • Análisis de cualquier software de tipo *open-source*, COTS(*Commercial off-the-shelf*) y *legacy* que sea parte del sistema, incluyendo la especificación de requisitos de resiliencia que tiene que cumplir cada software • Revisión de la especificación de los requisitos, incluyendo medidas para validad los niveles deseados o logrados de la resiliencia del software • Aseguramiento de la calidad durante la ingeniería de requisitos • Monitorizar y Auditar durante la ingeniería de requisitos • Mediciones durante la ingeniería de requisitos • Entrenamiento a los Ingenieros de Requisitos de Software Es importante considerar las prácticas de calidad que consideren en la organización para la ingeniería de requisitos, aunque se sugiere la norma ISO/IEC 9126-1:2001. *Software engineering -- Product quality* – y para la especificación de los requisitos la norma IEEE Std. 830-1998. IEEE *Recommended Practice for Software Requirements Specifications.*

		RTSE:SG1.SP3	**Identificar las directrices de Arquitectura y Diseño** El siguiente objetivo del ciclo de vida de desarrollo de software resiliente y una fase decisiva es la de la arquitectura y diseño. Esta práctica establece las directrices para diseñar resiliencia dentro del software y los sistemas. Una buena práctica en arquitectura y diseño hará que la implementación, montaje e integración del software se realice de manera óptima y que a nivel de resiliencia se haga sobre una base mucho más resiliente y resistente a interrupciones. Una especial atención en este proceso evitará dolores de cabeza a la hora de desarrollar cuando ya sea muy tarde implementar complementos para asegurar los requisitos establecidos. Una arquitectura y diseño resiliente basado en los requisitos definidos, protege y sostiene los servicios de acuerdo a los intereses de la organización, garantizando una respuesta adecuada a condiciones de interrupción y estrés. Las directrices de arquitectura y diseño para desarrollar software resiliente cubren los conceptos de diseño, arquitectura, diseño de componentes, diseño detallado y revisión y evaluación de diseño. Como producto tendremos unas directrices para el diseño y arquitectura de software y sistemas resilientes que se identificaran a través de: • Análisis de amenazas durante la arquitectura y diseño • Conjeturas, decisiones y fundamentos de diseño • *Attack Surface*, identificación de posibles alteraciones al software. • Métodos para representar perspectivas del defensor y el atacante, crear escenarios. • Patrones de diseño seguros a nivel de arquitectura y diseño • Control de Acceso • Gestión de Identidades • Seguridad de los Datos • Identificación y priorización de controles durante la arquitectura y diseño (CTRL) • Análisis de cualquier software de tipo open-source, COTS (*Commercial off-the-shelf*) y legacy, incluyendo la verificación de funcionalidades requeridas y comportamiento de resiliencia y ausencia de contenido malicioso. • Arquitecturas orientadas a servicios, virtualización y cloud computing (Software como Servicio) • Integración con arquitecturas existentes (Interconectividad e Interoperabilidad) • Análisis de riesgos durante la arquitectura y diseño • Análisis de la magnitud y complejidad del sistema, incluyendo los procesos de negocio de punta a punta y los análisis de fallos y vulnerabilidades del servicio • Inspecciones y revisiones de la arquitectura y el diseño, incluyendo validación de los niveles deseados o logrados de la resiliencia de software • Aseguramiento de la calidad durante la arquitectura y diseño • Monitorizar y Auditar durante la arquitectura y diseño • Mediciones durante la arquitectura y diseño • Entrenamiento a los arquitectos y diseñadores de software Para esto se sugiere apoyarse en la documentación de OWASP y la iniciativa SAMM de OWASP.
		RTSE:SG1.SP4	**Identificar las directrices de Implementación** La siguiente fase es la implementación, en la que se espera que se asegure que la resiliencia sea parte del ciclo de vida de codificación y pruebas del software. La idea es que se implementen todos los requisitos de resiliencia establecidos, como se ve reflejado en la arquitectura y diseño propuesto. Se debe trabajar bajo la premisa que un software resiliente es predecible en ejecución tanto en operación normal como en tiempo de estrés y que está libre de vulnerabilidades tanto como sea posible. Se deberán utilizar mejores prácticas tanto en la codificación como en las pruebas. Como producto tendremos unas directrices para la codificación de software resiliente, que a pesar de ser orientadas a proyecto se identificaran a través de: • Análisis de riesgos durante la codificación • Análisis de amenazas durante la codificación

			• Evaluación y Mitigación de *Attack Surface*.
			• Patrones de diseño seguros a nivel de implementación
			• Estándares de código seguro (Específicos del lenguaje)
			• Chequeos, inspecciones y revisiones del código y análisis estático y dinámico de código, incluyendo herramientas para soporte con el fin de verificar:
			  o Que se cumplen los requisitos de resiliencia
			  o Que se siguieron las directrices de arquitectura y diseño
			  o Ausencia de funciones prohibidas
			  o Ausencia de vulnerabilidades comúnmente conocidas
			  o Que se presenta el nivel deseado o logrado de resiliencia de software
			• Conducir revisiones más a fondo para los riesgos de mayor valor y códigos de mayor valor
			• Identificación y priorización de controles durante la codificación (CTRL)
			• Aseguramiento de la calidad durante la codificación
			• Monitorizar y Auditar durante la codificación
			• Mediciones durante la codificación
			• Entrenamiento a desarrolladores de software
			Además se deberán plantear unas directrices para la prueba de software resiliente, que a pesar de ser orientadas a proyecto se identificaran a través de
			• Análisis de riesgos durante las pruebas de software
			• Análisis de amenazas las pruebas de software
			• Reevaluación y Mitigación de *Attack Surface*.
			• A nivel de software, métodos para:
			  o Pruebas funcionales a requisitos de resiliencia
			  o Test de caja blanca, incluyendo análisis de cobertura de código
			  o Test de caja negra, que se enfoque en el comportamiento externo visible del software
			  o Fuzz testing
			  o Test de Penetración
			  o Test para vulnerabilidades específicas así como pruebas de regresión de vulnerabilidades
			  o Aplicación de modelos de amenaza y ataque
			  o Pruebas de software open-source, COTS y legacy, incluyendo la verificación de funcionalidades requeridas y comportamiento de resiliencia y ausencia de contenido malicioso
			  o Test de inspección en apoyo a la aprobación de entrega
			  o Test de regresión
			• Automatización de métodos y herramientas de prueba para apoyar la automatización
			• Revisiones de pruebas de software con el fin de verificar:
			  o Que se cumplen los requisitos de resiliencia
			  o Que se siguieron las directrices de arquitectura y diseño
			  o Ausencia de funciones prohibidas
			  o Ausencia de vulnerabilidades comúnmente conocidas
			  o Que se presenta el nivel deseado o logrado de resiliencia de software

			• Integridad y manejo de código (Incluyendo gestión de la configuración, cadena de custodia verificable, antifraude, monitoreo y análisis de eventos y logs de auditoría y firma de código) • Conducir revisiones más a fondo para los riesgos de mayor valor y códigos de mayor valor • Demostrar el cumplimiento con estándares de interoperabilidad (TM:SG5.SP4.) • Pruebas de controles durante las pruebas de software(CTRL) • Aseguramiento de la calidad durante las pruebas de software • Monitorizar y Auditar durante las pruebas de software • Mediciones durante las pruebas de software • Entrenamiento a Ingenieros de pruebas de software Para esto se sugiere apoyarse en la documentación de OWASP y la iniciativa SAMM de OWASP. Del mismo modo el uso de herramientas automatizadas que ya existen en el mercado para validación de códigos frente a vulnerabilidades.
		RTSE:SG1.SP5	**Identificar las directrices de Montaje e Integración** El software puede estar ligado a un sistema específico, por lo tanto su montaje e integración del software resiliente en sistemas resilientes tiene que definirse e identificarse. Para mantener la resiliencia del software, es necesario considerar que este será integrado a otros sistemas y que esto podrá afectar de manera significativa al entorno operacional de producción. Las vulnerabilidades pueden por varias razones, por tanto se deberán plantear las directrices que permitan hacer esto de la mejor manera. Tienen que ajustarse las formas de montaje e integración a las necesidades de negocio, a las mismas arquitecturas y considerar los escenarios que pueden influir, pues la resiliencia no es robusta si no se elabora una estrategia que permita mantener lo hecho en fases anteriores. El producto de esta práctica serán las directrices para el montaje e integración de las soluciones resilientes.
	RTSE:SG2	**RTSE:SG2.SP1**	**Seleccionar y ajustar directrices** Hay diversos tipos de software, e inclusive dentro de la misma organización alguno tendrá una función vital mientras otro puede rescindir de requisitos de resiliencia. Algunos necesitarán especial cuidado y requisitos específicos, en general dentro de la organización es un hecho que las directrices no aplicarán de manera estricta e igual a todo el software de la organización. Esta práctica dicta que se determinen las directrices para el proyecto de desarrollo de un software específico usando criterios de selección establecidos por la organización. Se tendrá en cuenta no solo el soporte a los servicios sino lo que nos ofrezca el área de proceso RRD. Una vez establecido el criterio se utilizará para seleccionar y ajustar las directrices de resiliencia para cada fase de ciclo de vida del proyecto software (RTSE:SG1). El producto de esta práctica serán los criterios de selección, las directrices de requisitos, arquitectura y diseño, implementación y montaje seleccionados. Se sugiere que los criterios de selección tengan en cuenta lo siguiente : • El valor de los servicios que el software planea soportar • El valor relativo del software de servicios que planea soportar • El grado en el cual el software maneja las acciones pedidas en los planes de mitigación de riesgo del servicio (junto con el correspondiente impacto y valoración del riesgo) • La prioridad de los requisitos y objetivos de resiliencia que deben ser satisfechos por el software • El análisis de compensación costo/beneficio, como la importancia relativa de identificar los defectos del software de manera temprana en el ciclo de vida del software frente al costo de implementar las directrices • Hacer análisis de compensación de la compra • La disponibilidad de personal debidamente capacitado • Los costos de capacitación del personal
		RTSE:SG2.SP2	**Integrar las directrices seleccionadas con un proceso definido de desarrollo de software y sistemas**

			Con las directrices definidas para cada fase del ciclo de vida, y seleccionadas para el software, ahora lo integraremos a un proceso definido de desarrollo de software y a un plan documentado. Las organizaciones que realizan la construcción de software, por lo general reúnen modelos y metodologías con el fin de definir, gestionar y mejorar un proceso para el desarrollo de aplicaciones. Muchas veces estas metodologías integran mejores prácticas de desarrollo y estimulan los procedimientos de calidad, pero dejan de lado consideraciones como la seguridad y la continuidad, es decir, dejan de lado la resiliencia. La consideración de esta práctica es integrar los procesos que establece la organización con las directrices seleccionadas, de modo que los sistemas cuenten con mejores prácticas de desarrollo, cumplan a cabalidad los requisitos funcionales, cuenten con propiedades de calidad, pero que también integren características de resiliencia definidas por la organización para interés de los servicios que se vayan a soportar. La idea es que el plan para un proyecto de desarrollo de un software específico se mejore y actualice con los requisitos y las directrices de resiliencia en las siguientes áreas: • Definición de los procesos de desarrollo • Tareas, medidas de progreso, hitos, entregables y la asignación de recursos (staff, capital, equipo, etc.) para implementar las directrices de resiliencia • Nuevos riesgos introducidos por las directrices de resiliencia y la elevación a una mayor prioridad de los riesgos actualmente identificados • Participación de los Stakeholder • Compromiso con el plan actualizado • Los criterios y autoridad de decisión en los principales hitos del proyecto Como producto de esta práctica tendremos las definiciones del proceso de desarrollo actualizado, igual que el plan de desarrollo.
	RTSE:SG3	**RTSE:SG3.SP1**	**Monitorear la ejecución del plan de desarrollo** El fin de esta práctica es asegurarse que se satisfacen los requisitos de resiliencia del software a través de la monitorización de la ejecución del plan de desarrollo. Debido a que el plan puede variar por diferentes condiciones, y que se pretende que en lo posible se mantenga la resiliencia, se monitorizará el proceso para asegurarse que el software satisface todos los requisitos definidos a un nivel apropiado de la fase del ciclo de vida. En caso que no se estén cumpliendo de manera satisfactoria los requisitos, los planes tendrán que ser actualizados y renegociados, y manejar el riesgo potencial y/o residual a través de RISK. La monitorización seguirá un proceso definido y estará ligada a la gestión de cambios establecida por la organización. Debería incluir coleccionar, analizar y reportar la efectividad de las directrices de resiliencia frente a cumplimiento, estado de los requisitos en cuanto a hitos planeados, identificación y planes de mitigación de riesgos, impactos a la continuidad del servicio para el software en desarrollo, impacto de los controles para proteger y sostener los servicios, software y sistemas, y mejoras a las directrices de resiliencia y definición de procesos que manejan la resiliencia. El producto de esta práctica será la definición de procedimientos para la revisión de los proyectos, medidas reportes y revisión de resultados del proyecto, actualización de los planes del proyecto, actualización de las directrices de resiliencia y de la definición de procesos.
		RTSE:SG3.SP2	**Entregar soluciones técnicas resilientes en producción** Una vez estamos seguros que el software cumple a cabalidad con los requisitos de resiliencia este puede ser entregado a producción, para esto tiene que comprobarse que se ha cumplido a satisfacción cada práctica anteriormente descrita. Antes de la entrega del activo software al entorno de producción operacional, estos activos deben ser sometidos a una inspección formal frente a los criterios documentados para asegurar que se han cumplido los requisitos de resistencia especificados. El resultado de los criterios de inspección satisfactorios es la aprobación para entregar el software a producción. Las prácticas sugeridas aquí son criterios, procedimientos y resultados de la inspección e implantación en entorno de producción con previo proceso de aprobación.

Tabla 18. Mapa de ruta para Software construido por externos basado en áreas de proceso CERT-RMM

5.1.3 Software adquirido

Área de Proceso	Metas	Prácticas	Recomendaciones
ADM	ADM:SG1	ADM:SG1.SP1	**Inventario de Activos** Es importante para la organización mantener de manera organizada sus activos, y del mismo modo se espera que la organización siga unas mejores prácticas en cuanto a la gestión de los mismos. Debido a que tratamos con software se debe tener en cuenta que al ser un activo intangible relacionado con tecnología, no tendrá un manejo igual al que tendrá un activo físico. De esta manera la gestión de TI debe asegure de establecer una adecuada gestión de activos de TI para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios, todo esto alineado con el marco de gobernanza de TI. En el caso del software adquirido se debe tener una administración completa y entendimiento de la gestión del producto. Un concepto importante es *Software Asset Management* (SAM), que corresponde a que a nivel de negocio se realice una adecuada gestión de la adquisición, mantenimiento, uso y disposición de las aplicaciones software dentro de la organización y la optimización de los procesos que se gestionan. Se sugiere utilizar marcos de gestión de software como ISO/IEC 19770 que se complementa con ISO 20000 en el proceso Gestión de la Configuración y en la cual la organización puede demostrar que realiza una gestión de activos de software. De igual manera ITILv3 incluye el proceso de Activos de Servicio y Gestión de la Configuración. COBIT 5 está alineado con ITILv3, por lo tanto puede considerar el inventario a alto nivel en la gestión de TI. Del mismo modo, SAM aporta a ISO/IEC 27002, en lo que a incidentes de seguridad de Software considera, es por esto que será un control preventivo a situaciones de interrupción o estrés. El producto de esta práctica debe ser un inventario y una base de datos del software de la organización. Del mismo modo se deberá identificar cuál software que se produce soporta procesos críticos del negocio y son vitales para la operación y la consecución de los objetivos de la organización. Se establecerá el valor de cada software que se produzca.
		ADM:SG1.SP2	**Establecer un Entendimiento Común** Es importante que se clasifiquen los activos software dentro de los activos de tecnología, del mismo modo, usando uno de los marcos sugeridos en ADM:SG1.SP1 se tendrá una buena práctica para que se manejen los activos de manera adecuada, y podrá ser el punto de partida para que se puedan asignar tanto a propietarios como vigilantes y entiendan sus responsabilidades (en la siguiente práctica ADM:SG1.SP3). El entendimiento será un punto de partida para evaluar las prioridades sobre los activos software en cuanto a resiliencia operacional, para saber cuáles tienen mayor valor para la organización en cuanto a resiliencia operacional no solo porque sean activos de alto valor sino también por los servicios que soporten, cuáles soportan servicios críticos y a partir de esto dará un enfoque global para establecer los requisitos de resiliencia. En este escenario, la organización tendrá que hacer énfasis en el proceso de adquisición, de modo que durante esta gestión se deje claras las responsabilidades y se tenga amplio entendimiento del soporte del software adquirido a los servicios, contando con especial atención en los servicios de alto valor. A través de esta práctica se llegará al entendimiento mutuo de los activos software y sobre todo cuáles son los de mayor importancia por soportar los servicios de la organización. Esto se puede realizar documentando la información necesaria, como políticas de uso, importancia y concienciación del activo frente a los servicios, entre otros.
		ADM:SG1.SP3	**Establecer Propietarios y Vigilantes** El software, como el resto de activos, tendrá asociados unos propietarios y unos vigilantes. Establecer mejores prácticas ADM:SG1.SP1 en general sobre los activos, y con un entendimiento común ADM:SG1.SP2 del aporte del software a la organización hará mucho más fácil establecer quién es quién dentro de las funciones del activo, y del mismo modo establecerá las pautas para la resiliencia operacional de la organización.

			Por un lado se establecerán los propietarios que tendrán la responsabilidad de la viabilidad, productividad y resiliencia del software, no necesariamente serán personas directamente, pueden ser unidades organizacionales internas teniendo en cuenta que la organización ya hizo la adquisición, y por ende es independiente de terceros. Por otro lado se establecerán vigilantes –que también serán personas o unidades organizacionales internas o externas– con la responsabilidad de implementar y gestionar los controles para satisfacer los requisitos de resiliencia, mientras estén a cargo del activo. Cabe resaltar que como se indicó anteriormente, en todos los casos, los propietarios son los responsables de asegurar la protección y continuidad apropiada de sus activos, sin tener en cuenta las acciones (o inacciones) de los vigilantes. El resultado de esta práctica será la identificación de los propietarios y los vigilantes y la actualización de los perfiles y las bases de datos de activos definidos. Es importante definir el perfil de propietario y vigilante y las responsabilidades que tienen con el software. En caso que el software soporte junto a un grupo de activos un servicio de la organización, es necesario establecer este grupo dentro de la identificación.
	ADM:SG2	**ADM:SG2.SP1**	**Asociar Activos con Servicios** Una práctica muy importante es empezar a establecer la relación de los activos con los servicios de la organización. Para una organización, asociar activos con los servicios es una práctica muy significativa debido a que es mucho más importante establecer resiliencia en un servicio de alto valor, que en un servicio complementario. La resiliencia operacional busca que la organización se enfoque en la visión de los servicios, debido a esto asociará el activo al servicio que soporta. En el caso del software, se tendrá clara no solo cuál será la funcionalidad –razón por la cual fue adquirido–, sino que se sabrá cuáles servicios van a asociarse y cuál será su rol para soportar el servicio. A partir de esta definición, será más fácil establecer las mejores estrategias en cuanto a protección y sostenimiento del software. Como resultado de esta práctica tendremos qué software se relaciona a los servicios de alto valor de la organización.
		ADM:SG2.SP2	**Analizar dependencias entre activos y servicios** Un activo puede soportar uno o más servicios, por esto se debe realizar un análisis general de estos servicios en la organización. Un CRM por ejemplo puede soportar varios servicios de la organización, y del funcionamiento de este podrán verse afectados uno o más servicios de alto valor. Una buena identificación de las dependencias es crucial pues será base para el establecimiento de los requisitos de resiliencia y por ende la estrategia de protección y sostenimiento del software. Como resultado de esta práctica evitaremos los conflictos potenciales por dependencias entre activos y se establecerán acciones y soluciones de mitigación.
	ADM:SG3	**ADM:SG3.SP1**	**Identificar Criterios de Cambios** (Esta práctica será complementaria a RRM:SG1.SP3) El ajuste a las necesidades de la organización y específicamente a los requisitos de resiliencia, afectará de manera directa al activo o a la asociación que tenga con un servicio, es por esto que se debe tener una práctica que sirva de soporte para el establecimiento y mantenimiento de los cambios. Los cambios identificados pueden afectar a uno o más activos, por esto las prácticas anteriores deberán soportar la estrategia de gestión del cambio establecida por la organización. En este caso los cambios estrictamente serán sobre el producto adquirido. Los propietarios serán directamente capaces de establecer la aplicación y gestión de los cambios sobre el software. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
		ADM:SG3.SP2	**Mantener Cambios a los Activos e Inventarios** (Esta práctica será complementaria a RRM:SG1.SP3) Así como se identifican los cambios, es necesario gestionarlos de manera adecuada, teniendo en cuenta los marcos de referencia que utilice la organización para el mantenimiento de cambios. Las condiciones de cambio, como serán sólo en la operación, es suficiente establecer procedimientos documentados de la gestión de cambios en el activo y que se tenga presente el estado del activo en ciertos instantes, de acorde a esto establecer los requisitos de resiliencia y la estrategia de protección y sostenimiento del software y de los servicios que soportan. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
EXD	**EXD:SG1**	**EXD:SG1.SP1**	**Identificar Dependencias externas** Este proceso es muy importante para este tipo de software. Cuando un tercero participa dentro de los procesos de la organización, la complejidad de las relaciones de la

			organización y los escenarios de riesgo aumentan. En este caso, construir, mantener o contratar software por un tercero. Estos terceros se considerarán dependencias externas, pues el activo –y el servicio– estará sujeto a las acciones de la entidad. Estas entidades tendrán que identificarse y priorizarse para asegurar la resiliencia de los servicios de alto valor que soportan, por lo tanto se identificará para entender, formalizar, monitorizar y gestionar los riesgos que esto ocasiona. Del mismo modo tener claro si soportan parte o todo un servicio y saber de qué activos son propietarios. Es importante recopilar toda la información, contratos entre proveedores, SLA, entre otros. El resultado de esta práctica será una lista detallada de las diferentes dependencias externas (descripción, activos y servicios que soportan, contratos,…), y un procedimiento documentado para la actualización de las mismas.
		EXD:SG1.SP2	**Priorizar dependencias externas** Es importante establecer prioridades sobre las entidades externas dependiendo de la importancia que tenga en la entrega de servicios de alto valor. Es importante realizar la priorización de dependencias externas pues la organización delega ciertas responsabilidades sobre los requisitos de resiliencia a dichas dependencias que manejan ciertos servicios, lo que le implica un papel importante para la consecución de la misión de la organización. El producto de esta práctica es establecer los criterios para priorizar estas entidades externas, y a partir de estos criterios se realizará la priorización de las dependencias externas, y los análisis de afinidad de las dependencias externas.
	EXD:SG2	**EXD:SG2.SP1**	**Identificar y evaluar riesgos debido a dependencias externas** Como se decía anteriormente, contratar una entidad externa aumenta la complejidad de las relaciones de la organización, pero también su entorno de riesgos. La gestión de riesgos de la organización juega un papel importante pues tiene que entender esa complejidad y ajustar la gestión a un número considerable de nuevos riesgos. Este proceso indica que se deben identificar y evaluar esos riesgos que se asumen al contratar a un tercero. Debido a que esto está involucrado en la gestión de riesgos se manejará en las prácticas RISK:SG3 y RISK:SG4. Por lo tanto el producto de esta práctica será las declaraciones de riesgos de dependencias externas con la evaluación de impacto y la lista de riesgos de las dependencias externas con categorización y priorización.
		EXD:SG2.SP2	**Mitigar riesgos debido a dependencias externas** La gestión de riesgos de la organización, entendiendo el nuevo escenario de riesgos que se crea, debe establecer e implementar las estrategias de mitigación, con el fin de mantener en un nivel aceptable de los riesgos derivados de las relaciones con dependencias externas. El producto de esta práctica serán los planes de mitigación de los riesgos de dependencias externas –donde se considera el desarrollo y revisión de controles– y la implementación y monitorización de la efectividad de los planes. Del mismo modo las prácticas serán complementadas por el proceso RISK:SG5.
	EXD:SG3	**EXD:SG3.SP1**	**Establecer especificaciones empresariales para dependencias externas** En general las relaciones con las entidades externas tienen que ser de tipo formal, a través de contratos o acuerdos que contribuyan seguridad al gobierno de la organización. Para escoger los proveedores, es necesario que estos demuestren que pueden cumplir lo que requiere la organización y que se ajustarán a las especificaciones del contrato. Al soportar servicios de la organización, las entidades externas se convierten en una extensión de la organización y la organización debe hacer que las entidades externas sean conscientes de la importancia de las políticas, estándares, lineamientos internos que a la larga son controles que ayudan a proteger y sostener las operación de la organización, siendo esto un apoyo para la resiliencia de la organización. Este pacto debe acordarse a nivel de empresa de modo que haya ese compromiso con la estrategia de resiliencia de la organización. Por esto a los externos se les compartirá los requisitos de resiliencia para que los tengan en cuenta RRD, y especificaciones referentes a los requisitos del software como tal (Por ejemplo, que el software se ajuste a los lineamientos establecidos por el Área de proceso RTSE, pues aunque no lo hace directamente se debe acordar que hayan prácticas como las ahí citadas). Como producto tendremos la lista de especificaciones de empresa que aplican a dependencias y entidades externas y las plantillas de acuerdo que reflejan las especificaciones empresariales.
		EXD:SG3.SP2	**Establecer especificaciones de resiliencia para dependencias externas** Así como a nivel de empresa se realiza este acuerdo, es necesario que se dejen claras las especificaciones de resiliencia que aplican para las entidades y

			dependencias externas. Una dependencia externa es el resultado del acceso de una entidad externa para controlar, desarrollar, poseer, ser responsable (de operación, mantenimiento o soporte), o tener obligaciones definidas relacionadas con uno o más activos o servicios de alto valor para la organización. Esos servicios tendrán unos requisitos de resiliencia y por ende la entidad externa tendrá un compromiso con el alcance de esos requisitos. Como producto de esta práctica se tendrán las especificaciones de resiliencia documentada y el acuerdo de nivel de servicio SLA. Es importante establecer comportamientos requeridos y normas de rendimiento esperados (disponibilidad, rendimiento, gestión del cambio, seguridad, continuidad del negocio…) con el fin de medir que se cumpla con los requisitos específicos
		EXD:SG3.SP3	**Evaluar y seleccionar entidades externas** Como se ha indicado, el proceso de elección de un tercero para realizar un proceso como en este caso construir/mantener/implantar/ofrecer software, debe ser estricto y tener como referencia unas especificaciones claves y unos criterios de selección adecuados. Las entidades externas son seleccionadas basadas en una evaluación de su habilidad de cumplir con las especificaciones establecidas en EXD:SG3.SP1 y EXD:SG3.SP2. Es decir, adicional al proceso de contrato, deberá tenerse en cuenta cumplir con las expectativas de resiliencia necesarias Como producto de estas prácticas se deberá establecer un proceso de selección que incluya los requisitos esperados (preferiblemente a través de documentos que comprueben la capacidad de cumplimiento), establecer criterios de selección, evaluar las propuestas frente a los criterios y tomar una decisión.
		EXD:SG3.SP4	**Formalizar relaciones** Una vez tomada la decisión, lo que queda es establecer y mantener un acuerdo formal con la organización que ofrece las mejores condiciones de servicio y que cumple con las expectativas de la organización. El acuerdo dependerá del servicio o producto que se contrate, dependerá de la relación entre las entidades, los niveles de integración. Como producto de esta práctica tendremos el acuerdo con la entidad externa. En este acuerdo deberán estar cuestiones documentales como términos, condiciones, especificaciones, entre otros, al igual que permisos, licencias y demás. Deberá incluir también los manejos de desarrollo del trabajo, especificaciones, estándares de desarrollo y prácticas a utilizar para mantener el servicio, seguridad, gestión de riesgos, estrategias de protección y sostenimiento de producto y proceso, … Y cuanta documentación y aclaración necesite estar documentada orientado a tener los términos del servicio claro.
	EXD:SG4	**EXD:SG4.SP1**	**Monitorear rendimiento de entidades externas** Para saber el rendimiento de la entidad externa la mejor manera es monitorizando su actividad y esto lo hará de acuerdo a las especificaciones establecidas, estas serán el resultado de EXD:SG3. Esto se hará de manera periódica para tener un registro y en ciertos casos tomar decisiones. Algunos criterios de medición serán los que se establezca en el acuerdo formal. En algunos casos, los cambios que se hagan y las decisiones también dependerá del ambiente cambiante de riesgos. Como producto de esta práctica tenemos los reportes de las entidades externas, las bases de datos de gestión de relaciones que nos muestra la información de la monitorización del rendimiento actual, y reportes de inspección de entregas de la entidad externa. La monitorización deberá ser un procedimiento conocido y con responsables.
		EXD:SG4.SP2	**Corregir rendimiento de entidades externas** Dependiendo de los resultados monitorización realizada, se llevarán a cabo acciones correctivas para apoyar el rendimiento de la entidad externa, esto es muy importante en un ciclo de mejora continua. Entre menos dependa de externos la continuidad de los servicios, mejor. Las acciones correctivas estarán en el acuerdo. Como productos de esta sección tenemos los reportes o documentación de acciones correctivas, estas se evalúan y se escogen las mejores acciones correctivas entre las alternativas propuestas, y se realiza una documentación con las acciones correctivas escogidas. Esto debe comunicarse a la entidad externa. Como es mejora continua vendrá la implementación, monitorización y actualización en caso que se requiera.
RISK	**RISK:SG1**	**RISK:SG1.SP1**	**Determinar las categorías y fuentes de Riesgo** Es necesario que se establezcan las fuentes de riesgo a las que se va a exponer el software, no solo como producto sino como proceso, y a partir de esto establecer las categorías y una taxonomía del riesgo operacional, que es el que implica directamente la operación habitual de los servicios. Identificar el riesgo es comprender a qué se enfrentará el software, y a pesar de no poder contar con todos los escenarios posibles ni blindar la operación a todas las amenazas, lo más importante es identificar lo más crítico y considerar los *Black Swan.* Hay que considerar las fuentes tanto internas como externas. La organización debe establecer un marco para la gestión de riesgos que tenga una visión holística del software, como se indicó en el Capítulo 2 seguir un estándar

			como ISO 31000 junto con mejores prácticas para el ciclo de vida del software (no solo del producto sino del proceso) nos ayudará a establecer lo que se espera de esta práctica, el riesgo operacional al que se expone el software, las categorías de riesgo y la taxonomía. Este marco de referencia será el apoyo para la definición de los requisitos de resiliencia.
		RISK:SG1.SP2	**Establecer una estrategia para la Gestión de Riesgo Operacional** La organización que cuenta con un marco para la gestión del riesgo empresarial ERM, generalmente cuenta con la base necesaria para establecer la gestión de riesgo operacional ORM. De acuerdo como decida la organización su estrategia a nivel ejecutivo, decidirá cuál será la estrategia a seguir para la ORM que cumpla con los objetivos del negocio. La estrategia que se establezca será la que defina el desarrollo de las actividades relacionadas con la ORM y la colección, coordinación y gestión de dichos riesgos al marco de procesos de ERM. Dentro de la estrategia se debe contar con que el software se adquiere, así que se debe considerar una taxonomía de riesgos que tenga en cuenta la adquisición y el mantenimiento del software, y se tendrá en cuenta la responsabilidad de terceros en el escenario de riesgos y del mismo modo habrá una delegación de responsabilidades en la gestión de riesgos. La estrategia debe estar documentada y comunicada a todos los interesados internos y externos responsables de las actividades de ORM, de modo que se tenga el entendimiento y sirva de entrada para otros procesos –por ejemplo para definir los requisitos de resiliencia.
	RISK:SG2	**RISK:SG2.SP1**	**Definir los parámetros de Riesgo** Para evaluar la relevancia del riesgo operacional en la organización, es preciso establecer unos parámetros con los cuales se pueda medir, es decir, se tenga una fotografía del estado actual de la organización. Para esto se definirán unos umbrales de tolerancia de riesgo que reflejará el nivel de riesgo dispuesto a admitir y a enfrentar la organización. Este deberá considerar que el riesgo implicará el producto y que toda la gestión será por parte de la organización. Con un marco de gestión de riesgos, es claro que se establecerán estas medidas, y que acorde a la estrategia y objetivos de la organización se dictarán los parámetros a los que quiere apuntar y con los que evaluará el riesgo operacional, y con los cuáles definirá los requisitos para la gestión de riesgos.
		RISK:SG2.SP2	**Establecer criterios de medida del riesgo** Así como se definen los parámetros, es necesario definir los criterios para medir el impacto del riesgo dentro de la organización. Estos criterios serán importantes para clasificar, evaluar y priorizar los riesgos operacionales. El producto de esta práctica es el conocimiento de las áreas de impacto –donde el riesgo material tiene consecuencias significativas e interruptivas– priorización de dichas áreas y un documento con los criterios de medida y evaluación y con la probabilidad de riesgos.
	RISK:SG3	**RISK:SG3.SP1**	**Identificar los Niveles de riesgo en los Activos** Antes de establecer resiliencia operacional sobre los activos, es preciso que se tenga claro que los activos y por ende servicios se pueden ver afectados por los riesgos operacionales, por lo tanto su identificación y mitigación es primordial. Acorde a las categorías y al nivel de riesgo definidos por la organización, se identificarán los riesgos que afecten a los activos. Eso sí, es claro que no se identificará la totalidad de riesgos, pero al menos los riesgos operacionales que afecten los servicios, estos deben ser identificados y gestionados a través de diferentes técnicas. De ahí la importancia de seguir uno de los marcos para la gestión de riesgos. Deberá considerarse los escenarios en los cuales la gestión sea por parte de la organización y que el software adquirido se vea expuesto. Como producto de esta práctica, tendremos un conjunto de herramientas para la identificación del riesgo organizacional, y una lista de riesgos categorizados por activo.
		RISK:SG3.SP2	**Identificar los Niveles de riesgo en los Servicios** El objeto de establecer la resiliencia operacional, es garantizar que los servicios cumplan la misión, sin embargo estos servicios están expuestos a unos riesgos operacionales que son el resultado de una serie de riesgos sobre los activos de la organización. Por esta razón hay que evaluarse el impacto potencial de un riesgo sobre un activo, en este caso los riesgos sobre el producto software sobre su funcionamiento, y su impacto sobre la misión del servicio. De acuerdo a esto no solo se puede mitigar sino priorizar teniendo en cuenta los intereses de la organización. Se asume que la organización identificó de manera esencial los servicios de alto valor, y en el proceso ADM los activos asociados a estos servicios. Como resultado de esto podremos clasificar los riesgos por servicio y establecer contextos donde afecta el servicio y consecuencias de los riesgos sobre los servicios si se llegan a materializar.

	RISK:SG4	**RISK:SG4.SP1**	**Evaluar Riesgos** Teniendo como lineamiento las prácticas realizadas anteriormente para la medición del riesgo (tolerancia, criterios e impactos del riesgo), lo siguiente es evaluar el riesgo operacional y sus consecuencias. Los riesgos varían en cada caso y específicamente para el software tenemos que considerar los diversos escenarios a los cuales esté expuesto el proceso. Esta evaluación nos dará una idea de cómo manejaremos el impacto de los riesgos y cómo actuar en diversas circunstancias operativas. El producto de esta práctica será la evaluación con base a los lineamientos de la organización y darle un valor cualitativo para poder decidir cómo actuar, y cómo priorizarlos.
		RISK:SG4.SP2	**Categorizar y Priorizar Riesgos** Una vez evaluados, podemos categorizar los riesgos operacionales de modo que establezcamos las prioridades sobre las actuaciones que se vayan a realizar sobre los mismos. Las categorías dependerán de los intereses, pero hay diferentes maneras de categorizas, por fuentes, por nivel de riesgo, por taxonomía, etc. Es importante tener en cuenta los escenarios y no olvidar los *Black Swan*, que en muchos casos son causas drásticas de interrupción o estrés del servicio. La priorización será importante a la hora de establecer resiliencia. Como resultado de esta práctica tendremos los riesgos por categorías y con priorización, de acuerdo a los intereses de la organización.
		RISK:SG4.SP3	**Asignar disposición al Riesgo** Del mismo modo que la organización asume que hay entendimiento de los riesgos, puesto que de acuerdo a su postura se evalúa, tiene también que documentar y aprobar su posición frente a los escenarios de riesgo identificados. Las acciones que tome de acuerdo a los riesgos tendrán que ser el producto de la estrategia establecida en la gestión de riesgos. La organización puede tomar diferentes disposiciones, entre ellas evitar el riesgo, aceptar el riesgo, transferir el riesgo o mitigar y controlar. Como producto de esta práctica de deberá listar los riesgos y la disposición de la organización, y los riesgos priorizados para mitigar. La disposición al riesgo será documentada y debidamente aprobada por la organización (en especial con los riesgos que se aceptarán).
	RISK:SG5	**RISK:SG5.SP1**	**Desarrollar planes para la mitigación del riesgo** Es necesario que se desarrollen planes de mitigación, sobre todo cuando el riesgo, producto de la evaluación realizada, está sobre el umbral y es inaceptable de admitir, no se desea transferir, y evitar solo sea posible eliminando la actividad que lo genera. La mitigación del riesgo puede requerir actividades referentes a la protección y sostenimiento del activo, o en algunos casos implementación de controles. En algunos casos las actividades no son suficientes y se deberá considerar el riesgo residual. Como práctica resultante tendremos el plan de mitigación del riesgo, para todos los riesgos a los que se dispuso mitigar y controlar. En este plan debe estar claro cómo se reduce la amenaza o cómo se protege la vulnerabilidad, las acciones preventivas, los controles a implementar, los planes de continuidad del servicio y los responsables del mismo, el costo del plan, manejo del riesgo residual.
		RISK:SG5.SP2	**Implementar estrategias de Riesgo** La organización toma una posición frente a los riesgos, y se espera que las estrategias que establece en la gestión de riesgos se sigan durante el todo el proceso, es por esto que los planes y estrategias de mitigación de riesgos serán implementados y además monitorizados. Lo que se gana con este ciclo continuo es que en un entorno cambiante de riesgos, debido a las nuevas condiciones de complejidad que se ve en las organizaciones de hoy en día, se tenga claro que la estrategia esté bien dirigida y los riesgos bien identificados, y en caso de cambios se revise y se modifique. El producto de esta práctica será la documentación de la implementación del plan de mitigación, y una visión actualizada del estado de los riesgos de acuerdo a la efectividad de la mitigación frente a las condiciones actuales, a través de la monitorización y unas políticas de seguimiento.
	RISK:SG6	**RISK:SG6.SP1**	**Revisar y ajustar estrategias para proteger los activos y servicios** Una de las formas de gestionar el riesgo operacional es la protección de activos y servicios, por lo tanto los controles que se implementen con este fin deben ser evaluados constantemente y actualizados según se requiera con base en la información que proporcione el riesgo. Los controles serán el resultado del proceso de gestión de riesgo o de los requisitos de resiliencia, la experiencia de la organización es la que le dará la madurez de la definición de estos controles, mejorar los actuales e implementar los que necesite, así como la consideración de controles que podrán proteger los activos y servicios de situaciones de riesgo emergentes. El producto de esta práctica será la lista de controles a revisar, mejorar o desarrollar y un plan de revisión.

		RISK:SG6.SP2	**Revisar y ajustar estrategias para sostener los activos y servicios** La otra forma de gestionar el riesgo operacional es el sostenimiento de activos y servicios, por lo tanto las estrategias de continuidad del servicio serán fundamentales de acuerdo al análisis que se realice en caso que el riesgo se materialice. Para esto se plantean planes de continuidad del servicio. Basado en la información de riesgo y lo aprendido en el ciclo de vida del riesgo, se pueden identificar falencias en la definición de los planes a través de las revisiones y posteriormente proponer mejoras. La validación de los planes será una manera de saber su efectividad frente a riesgos o amenazas operacionales El producto de esta práctica será la lista de planes de continuidad del servicio a revisar, mejorar o desarrollar y un plan de revisión.
RDD	**RRD:SG1**	**RRD:SG1.SP1**	**Establecer Requisitos de Resiliencia Empresarial** La organización a nivel de empresa, debe definir los requisitos de resiliencia con base a lo que necesite, generalmente motivados por la estrategia o cuestiones de cumplimiento. Debido a que el software es un activo de tipo "tecnología", los requisitos que se tendrán en cuenta son los que están ligados a la integridad y disponibilidad, si hace parte de un grupo de activos podrá también considerarse la confidencialidad. Como producto de esta práctica tenemos la lista de requisitos de resiliencia que define la empresa, que son el producto de la estrategia, objetivos, leyes, reglas y políticas, deberán tenerse en cuenta en el proceso de adquisición.
	RRD:SG2	**RRD:SG2.SP1**	**Establecer Requisitos de Resiliencia de Activos** Una vez teniendo conciencia de los requisitos de empresa con los que se verá afectado el software, se tendrá que tener en cuenta como tal los requisitos de resiliencia que conciernen directamente al software. Es claro que estos requisitos se definirán con base en los servicios de alto valor que desee proteger y sostener la organización y por ende al activo que lo soporte, que para este caso es el software. Por tanto en esta práctica se deberá hacer una lista de lo que se considera en la organización como servicio de alto valor, establecer las relaciones entre servicios, procesos de negocio y para este caso específico el software asociado, y la lista de requisitos de resiliencia por cada software de la organización que esté asociado con un servicio de alto valor. Ya que hablamos de software, es importante que se realice una buena práctica para la ingeniería de requisitos, de modo que el software que se adquiera, cumpla con los requisitos que la organización establece y que mantenga la resiliencia operacional de la organización. Teniendo ya asociados unos propietarios (proceso ADM) y con buena parte de la evaluación de riesgos (RISK), esta identificación tiene una entrada de información significativa
		RRD:SG2.SP2	**Asignar Requisitos de Resiliencia Empresarial a los Servicios** Los requisitos de resiliencia que afectan los servicios deberán ser asignados a los servicios. Aquí se establecerá la relación necesaria para identificar la colección de requisitos de resiliencia para los servicios, a través de la asociación entre misión de empresa-misión de servicio-activo asociado. El producto de esta práctica es asociada a la lista de RRD:SG1.SP1y RRD:SG1.SP2 y tendrá en cuenta los servicios relevantes junto con los requisitos de resiliencia específicos por servicio. Con esto se identifica y asignan los requisitos aplicables bajo la relación requisito empresa -requisito de servicio-requisito de activo. Esto será de gran ayuda para establecer la relación del activo software con los requisitos de los servicios y la estrategia de resiliencia operacional de la organización.
	RRD:SG3	**RRD:SG3.SP1**	**Establecer una definición de la funcionalidad requerida** La organización debe tener definidas las funcionalidades requeridas de un activo en el contexto del servicio, por lo tanto es tener clara la funcionalidad que el software va a proporcionarle al servicio de la organización y cómo se va a mantener el software a través del ciclo de vida. Realizar una monitorización de esto proporciona una entrada para el análisis y validación de los requisitos de resiliencia a nivel de activo. Esta hace parte de la descripción del activo que se hará en ADM y estará documentada.
		RRD:SG3.SP2	**Analizar Requisitos de Resiliencia** Es claro que los requisitos de resiliencia buscan proteger y sostener los servicios, sin embargo también es de resaltar que en una organización hay requisitos que dependen de otros requisitos, o que tal vez un requisito entre en conflicto con otro que es prioritario. Lo que busca esta meta es que se analicen los conflictos que hay en los requisitos, si hay conflictos realizar planes de mitigación a los conflictos, y esto hacerlo a nivel

			de los activos, en este caso software. La definición de funcionalidad junto con el análisis de requisitos a nivel de activos nos puede dar una idea de los conflictos, y con base a esto se pueden hacer los ajustes necesarios y desarrollar los planes de mitigación para resolver los conflictos. Estas definiciones ayudarán al entendimiento de cómo el software adquirido afectará los requisitos de resiliencia de empresa y de otros activos, entre ellos otras aplicaciones de la organización. Esto deberá tenerse en cuenta en la adquisición e implementación del software.
		RRD:SG3.SP3	**Validar Requisitos de Resiliencia** Teniendo una consistencia en los requisitos de resiliencia a nivel de activo, podemos decir que cumple con las expectativas de protección y sostenimiento que se necesitan, y si se asegura a este nivel, tendremos resiliencia en los servicios y en la operación de la organización. Con lo que proporciona RISK, tenemos que asegurarnos que hay requisitos de protección y sostenimiento tanto para el software como para su proceso de adquisición y mantenimiento. Del mismo modo, esta práctica busca optimizar los requisitos realizando una revisión en la que se detectarán los vacíos y con esto las actualizaciones o mejoras en los requisitos y en las medidas a implantar. De este modo, esta práctica proporciona un análisis entre objetivos estratégicos y requisitos de activos y un análisis de requisitos para asegurarse de qué se necesita para proteger y sostener el activo en relación con el servicio.
RMM	**RRM:SG1**	**RRM:SG1.SP1**	**Obtener un entendimiento de los Requisitos de Resiliencia** En el área de proceso RRD ya se establecen y definen los requisitos, de modo que ahora se deben entender, es decir que todos los propietarios de los servicios y los vigilantes y propietarios de los activos entiendan su rol y responsabilidad dentro de la implantación de la resiliencia en la organización. Para esto el área de proceso ADM tendrá un papel muy importante. Como se indicó anteriormente, en gran parte el propietario del activo tendrá que definir cuáles son los requisitos de resiliencia, en este caso el software. Esto lo hará basado en el entendimiento de la motivación de la organización y la búsqueda de la protección y sostenimiento del activo. Del mismo modo tendrá que tener en cuenta los requisitos de empresa y los análisis de la evaluación e impacto de los riesgos. Como producto de esta práctica tendremos los criterios de evaluación y aceptación de los requisitos por los vigilantes, y un acuerdo entre los propietarios y vigilantes del activo de mantener el conjunto de requisitos establecidos.
		RRM:SG1.SP2	**Obtener un compromiso con los Requisitos de Resiliencia** Es necesario que además de entender, haya un compromiso para la implementación de los requisitos establecidos. En esta práctica es significativo que la comunicación a los vigilantes, pues ellos estarán en contacto permanente y podrán entender lo que necesitan asegurar para el activo, por lo tanto se les debe comunicar lo que necesitan saber y que ellos hagan ese compromiso de implantar y mejorar los requisitos. Los propietarios serán los encargados de monitorizar y mejorar lo que suceda durante el ciclo de vida del activo. Como producto de esta práctica tenemos los compromisos documentados de requisitos y cambios en los requisitos, esto puede estar, por ejemplo en el acuerdo de nivel de servicio SLA.
		RRM:SG1.SP3	**Gestionar los cambios en los Requisitos de Resiliencia** La práctica anterior pide que se documente los compromisos en los cambios de los requisitos, esta práctica establece que haya un proceso definido de gestión para esos cambios. Es claro que las condiciones actuales de las organizaciones hacen que los escenarios de riesgo cambien y así mismo los requisitos de resiliencia, es por eso que se debe establecer este proceso que dicte los lineamientos para identificar y gestionar cambios. Se recomienda alinear la gestión del cambio con el marco que se implemente en la gestión de servicio de TI, bien sea ITIL o ISO 20000, y del mismo modo establecer los responsables y aprobadores de cambios. Como producto de esta práctica tendremos la base, el estatus, la base de datos –incluyendo historial de cambios, los criterios de cambio y peticiones de cambio de los requisitos.
		RRM:SG1.SP4	**Mantener la trazabilidad de los Requisitos de Resiliencia** Es importante seguir el ciclo de vida de los requisitos, su desarrollo, implementación y monitorización. La organización tiene que estar al tanto que las necesidades que tenía y que tradujo en requisitos, son satisfechas por las actividades propuestas. Es muy importante tener en cuenta el área de proceso RRD, pues teniendo claro los requisitos podemos realizar una matriz de trazabilidad y proponer un sistema para el seguimiento de los requisitos, con esto no solo conoceremos los activos que se relacionan sino con esto manejaremos los conflictos, y tendremos mucho más presente las interdependencias (Es claro que el software podrá soportar uno o más servicios de alto valor, o será parte de un grupo que soporte uno o más servicios)

		RRM:SG1.SP5	**Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos** Realizar la trazabilidad de la práctica anterior nos puede ayudar a la identificación y gestión de las inconsistencias entre requisitos y actividades, la idea es garantizar que se cumplen los compromisos con los requisitos y las actividades a desarrollar con el fin de garantizar la implementación de la resiliencia en la organización. En algunos casos a pesar de los esfuerzos, algunos requisitos no se cumplen porque dependen de más de un activo, en este caso se debe identificar y documentar esas inconsistencias para poder realizar las acciones correctivas pertinentes. Por esta razón se sugiere hacer revisiones de consistencia entre actividades y requisitos.
CTRL	**CTRL:SG1**	**CTRL:SG1.SP1**	**Definir los objetivos de control** Los objetivos de control son una manera de evaluar el rendimiento del sistema de control interno de la organización, sirve para garantizar un nivel apropiado de controles que le ayuden conseguir los objetivos estratégicos. Se pueden establecer objetivos de control, en TI por ejemplo, para asegurarse que el software y los sistemas consiguen los objetivos de una manera segura, eficaz y eficiente con un alto grado de protección y sostenimiento de un servicio de alto valor. Un ejemplo es el uso de objetivos de control es COBIT, para la gestión de TI. Pero así como definen algo general pueden llegar a definir algo específico. Es por esto que la definición es muy importante, pues para este caso de gestión de la resiliencia operacional, específicamente la resiliencia del software, los objetivos de control se definen en relación con los objetivos estratégicos de la organización, la información adquirida en RISK y en RRD. Los objetivos de control apuntarán a las estrategias de protección y sostenimiento de los activos relacionados con los servicios para asegurarse de que se gestiona su exposición a vulnerabilidades y amenazas. Con base en estos objetivos de control y las estrategias de protección y sostenimiento, se seleccionarán, analizarán y gestionarán los controles específicos. Como producto de esta práctica tendremos las directrices para la selección de los objetivos de control, los objetivos de control como tal, criterios para la priorización y lista de objetivos de control. Esto será importante a nivel general para establecer responsabilidades en la organización con base en los marcos de gestión como COBIT.
	CTRL:SG2	**CTRL:SG2.SP1**	**Definir los controles** Teniendo como referencia los objetivos de control y las estrategias de protección y sostenimiento de los servicios y activos de alto valor, se definirán los controles. Los controles no son necesariamente tecnológicos (Usando prácticas de *Secure Coding* nos ayuda a asegurar el producto, no necesariamente el proceso de implantación o entrega). Un control será una política, procedimiento, método, metodología, tecnología o herramienta que satisface un objetivo de control. Los controles que interesan a la gestión de resiliencia operacional son los que reducen la exposición a amenazas o vulnerabilidades que afectan a los activos y de este modo a los servicios y que ayudan a que esos mismos servicios y activos respondan y se recuperen mientras están en estado de interrupción. Estos controles podrán ser administrativos, técnicos o físicos a nivel general, y por su naturaleza preventivos (Separación de responsabilidades, documentación adecuada,…), detectivos (monitorización, auditorías,..), compensativos o correctivos. La práctica de esta parte es el listado de controles que protegen los servicios y activos. Controles a nivel de empresa, controles a nivel de servicio y activo y una matriz entre objetivos de control y controles (como la que ofrece COBIT). Del mismo modo asignar responsables para su implementación. Como estamos hablando específicamente de software, los controles específicos de producto son los que se implementen en el proceso TM.
	CTRL:SG3	**CTRL:SG3.SP1**	**Analizar los controles** Como una práctica ya conocida, es necesario realizar el análisis de los controles existentes, de modo que los controles concuerden con los requisitos de resiliencia y ayuden al logro de los objetivos de control. Adicionalmente es una oportunidad de considerar más controles, Como resultado de esta práctica encontramos el análisis de resultados, los objetivos que se satisfacen por los controles, vacíos en los controles, mejoras necesarias, controles propuestos, riesgos relacionados con objetivos de control no cubiertos y riesgos relacionados con riesgos redundantes y/o conflictivos
	CTRL:SG4	**CTRL:SG4.SP1**	**Evaluar los controles** Una vez hecho el análisis, es preciso evaluar si los controles satisfacen los requisitos de resiliencia establecidos. Esta es una manera de medir la efectividad de los controles de acuerdo a la iniciativa de resiliencia que tiene la organización. Esta evaluación debe hacerse de manera periódica, para poder mantener la gestión de los objetivos de control que estén orientados a la protección y sostenimiento de los servicios. El producto de esta práctica será la evaluación de los controles que contará con un alcance, unos resultados, áreas de problema, mejoras o actualizaciones a los controles existentes, nuevos controles propuestos, planes de remedio, actualizaciones a los planes de continuidad y riesgos relacionados a problemas sin resolver.
SC	**SC:SG1**	**SC:SG1.SP1**	**Planear la continuidad del servicio**

			En la tarea de proteger y sostener los activos, específicamente el sostenimiento dependerá de una estrategia efectiva de la continuidad del servicio. La organización debe enmarcar una estrategia de continuidad del negocio, y esta orientará la estrategia de la continuidad del servicio y su gestión para los procesos destinados a la planeación y ejecución de la sostenibilidad. LA idea es garantizar que los servicios de alto valor alcanzan la misión del servicio a pesar de situaciones de estrés y/o interrupción. Como primera medida se deberá elaborar el plan de continuidad del servicio para su desarrollo e implementación en los procesos de continuidad de servicio de la organización. La planeación mostrará el cómo la organización va a manejar la continuidad del servicio, y esto será una de las bases de la resiliencia operacional. El producto de esta práctica será el plan para la gestión de la continuidad del servicio –donde deberá estar alineado con: la posición de la organización frente a la continuidad del servicio; con la estructura del programa y los procesos de continuidad del servicio; con los requisitos relativos a la gestión de la resiliencia operacional del programa de continuidad del servicio; con los medios y las actividades relacionadas con la identificación y priorización de los servicios y activos para la continuidad; con las funciones y responsabilidades necesarias para llevar a cabo el plan y el programa; con las necesidades y requisitos de formación aplicables; con los recursos que serán necesarios para cumplir con los objetivos del plan; con los costos y presupuestos relevantes asociados a la continuidad del servicio. Y como es fundamental las peticiones de compromiso y el compromiso como tal que se haga con el plan deben estar documentados.
		SC:SG1.SP2	**Establecer estándares y directrices para la continuidad del servicio** Debido a la importancia de la continuidad del servicio, no se debe dejar de lado la implementación de mejores prácticas y aprender de los casos de éxito, por esto es necesario establecer y comunicar los estándares y directrices para la continuidad del servicio. Esto debe estar orientado a los objetivos de la organización. El producto serán las normas y directrices para la gestión de la continuidad del servicio. Estos serán desarrollados y comunicados resaltando responsabilidades, requisitos, entregas documentadas, modelo del contenido del plan, prueba de requisitos, y lo que se considere necesario para dejar claro el plan.
	SC:SG2	**SC:SG2.SP1**	**Identificar los servicios de alto valor para la organización** Para saber cuáles son los servicios a considerar, es necesario identificar y priorizar aquellos que son de alto valor, es decir aquellos que se requieren para que se cumpla la misión de la organización. Identificando estos servicios, será posible identificar el alcance y el tipo de plan de continuidad del servicio que se debe desarrollar e implementar. La idea es identificar los servicios de alto valor para la organización y sus activos asociados, esto puede basarse en lo que se defina en ADM En un marco de gestión de TI es claro que se tendrá claro cuáles son los objetivos de la empresa que se ven soportados por un servicio y que a su vez será un servicio de alto valor apoyado por un activo software. El resultado es la priorización de los servicios, actividades y activos asociados de alto valor (Apoyado por ADM). Igualmente los resultados de la evaluación de los riesgos en seguridad (Apoyado por RISK) y análisis de impacto en el negocio.
		SC:SG2.SP2	**Identificar dependencias e interdependencias internas y externas** Es claro que con el aumento de complejidad en las relaciones de las organizaciones, la resiliencia operacional cambia, por eso es importante para identificar y analizar las dependencias internas y externas y las interdependencias con el fin de asegurar la continuidad de servicio. En el caso de estudio deberá dejarse claras las responsabilidades de terceros sobre los servicios de la organización, manejar las relaciones y establecer responsabilidades. Como producto tendremos los proveedores de servicio de los cuales se depende, la lista de entidades externas que están incluidas en la entrega del servicio. El proceso ADM nos ayudará a identificar el activo que dependa de manera externa y la gestión con el área de proceso EXD.
		SC:SG2.SP3	**Identificar los registros y bases de datos organizacionales vitales** Una de los aspectos más importantes para la organización, y que está recogido en otra área de proceso CERT-RMM (*Knowledge and Information Management*) y que no tendremos en cuenta para esta guía es la resiliencia de la información. Para la organización la información es de vital importancia y mucho más si contribuye a los aspectos de la resiliencia operacional. Es por esto que se debe identificar la información vital requerida para la continuidad del servicio. Por lo tanto se deberán identificar y documentar los registros y bases de datos vitales, el personal fundamental y sus funciones específicas en el aprovisionamiento de los servicios, y asegurarse que los registros y bases de datos sean protegidos, accesibles y usables si ocurre una interrupción. A pesar que no concierne directamente a una medida a implementar en el software, si es una realidad que la información será importante en los sistemas resilientes.
	SC:SG3	**SC:SG3.SP1**	**Identificar los planes a ser desarrollados** Una vez establecido, se debe identificar cuáles son los planes de continuidad de servicio requeridos y que serán desarrollados, probados, ejecutados y mantenidos. Este deberá tenerse en cuenta durante el diseño e implementación de requisitos de resiliencia sobre los servicios y activos, es decir que para el software será importante que se

			tenga un trabajo paralelo en cuanto al plan y el soporte de los servicios o servicio al que vaya a soportar. Igualmente en este estará el resultado de las evaluaciones de riesgos en seguridad, las estimaciones del impacto, los requisitos de cumplimiento y considerando los Black Swan y las catástrofes.
		SC:SG3.SP2	**Desarrollar y documentar los planes de continuidad del servicio** Una vez identificados, se deben desarrollar y documentar los planes requeridos para la continuidad del servicio. Este se deberá realizar con base a los estándares y lineamientos establecidos. El software toma relevancia porque el personal de TI se involucra de manera significativa en el desarrollo y documentación del plan, en especial por los servicios que son automatizados o tienen una o más aplicaciones asociadas. Con el personal de TI y los propietarios del servicio en el equipo que elaborará los planes de continuidad, la resiliencia en el software será decisiva no solo por un servicio software directamente sino por otro tipo de servicios que puede soportar. Esta práctica nos dará como resultado las plantillas de los planes y los planes como tal para la continuidad del servicio. Dentro de esto deben recogerse los aspectos claves (p. ej. Actividades alternativas a desarrollar, recursos alternativos, activos de alto valor necesarios para soportar el plan), responsables e interesados.(Sobre todo si se implican terceros tener presente EXD), y cuestiones legales y de cumplimiento (p.ej. preparación frente a amenazas naturales o terrorismo)
		SC:SG3.SP3	**Asignar personal a los planes de continuidad del servicio** Para tener la certeza que el plan se ejecutará de manera eficaz, es necesario asignar miembros del personal a los planes de continuidad del servicio Al asignar personal, se deberá escoger personal que tenga las habilidades y responsabilidad de responder durante la ejecución del plan. Dependiendo del caso el personal será interno o externo (dependerá de contrato y SLA). Como producto de esta práctica tendremos los requisitos de personal a involucrar en el plan de continuidad del servicio, y la lista de miembros potenciales del personal. Una vez con esto queda asignar tareas al personal relacionado y establecer compromisos con las personas designadas. La organización se encargará también de la concienciación y formación del equipo.
		SC:SG3.SP4	**Almacenar y asegurar los planes de continuidad del servicio** Los planes de continuidad del servicio deben ser almacenados y accesibles a aquellos que lo necesiten, del mismo tienen que protegerse a través de controles de acceso que asegure que será accedido solo por aquel que sea autorizado
		SC:SG3.SP5	**Desarrollar el plan de formación para la continuidad del servicio** Para que un plan o una política tengan efecto en la organización hay que capacitar al personal, no solo del equipo sino general. Por lo tanto hay que desarrollar y administrar el entrenamiento en el plan de continuidad del servicio. Es importante que todos los involucrados en el plan tengan claras sus funciones y las responsabilidades que les competen. En algunos casos sirve para detectar vacíos de responsabilidad o habilidad en el personal. De esta práctica tendremos la lista de necesidades y vacíos del personal, una estrategia, unos materiales, unos registros y una retroalimentación de la evaluación de entrenamiento en el plan.
	SC:SG4	**SC:SG4.SP1**	**Validar los planes con requisitos y estándares** El fin de revisar el plan es que se satisfagan los requisitos y las necesidades de la organización en cuanto a resiliencia, por esta razón se tendrán que revisar los planes. Los planes de continuidad del servicio deben ser validados de modo que se eviten conflictos en el plan, que se compruebe que está alineado con lo que define la organización (estándares y directrices) y que se implementan los requisitos que establece RRD y RRM. Para esto se elabora una lista de requisitos que no se han cumplido, problemas de contenido y preocupaciones del plan, y un plan de actualizaciones y de medidas de remedio (los riesgos expuestos serán parte de RISK).
		SC:SG4.SP2	**Identificar y resolver los conflictos del plan** Debido a que hablamos de resiliencia operacional de la organización es normal que existan conflictos entre el mismo plan, debido a la cantidad de relaciones entre los activos, por esta razón se deberán identificar y resolver los conflictos, eso sí, bajo los parámetros de gestión del cambio que maneje la organización. En dado caso habrá que revisar o reescribir el plan.
	SC:SG5	**SC:SG5.SP1**	**Desarrollar programas y normas de pruebas** Lo que nos queda será probar el plan de continuidad del servicio, por lo tanto se deberá establecer e implementar un programa y unas normas para las pruebas. La organización deberá realizar estas pruebas en entornos controlados para asegurarse que el plan funciona y que cumple con su labor. Se debe establecer un programa, unas normas y unas fechas que permita saber que el software que soporta los servicios reaccionará ante las amenazas que se prevén en RISK y que se ven contempladas en

			RRD. Como resultado tendremos el programa y normas para los test considerando aspectos como estrategia de la organización, establecimiento de objetivos de calidad del test, nivel de involucre y compromiso de los interesados, reportes, revisión de aseguramiento de la calidad, directrices para manejar los problemas y directrices para la frecuencia
		SC:SG5.SP2	**Desarrollar y documentar planes de prueba** Una vez tenemos la referencia de los lineamientos, se desarrollaran y documentaran los planes de pruebas de continuidad del servicio. La importancia de documentar los procesos es que queda claro el guion, tanto lo que se quiere como los que participan, sus funciones, y los procedimientos. Se debe también tener en cuenta el entorno y tener muy claros los objetivos del test. Como resultado tendremos los planes para probar el plan de continuidad del servicio.
		SC:SG5.SP3	**Ejercer planes** Una vez teniendo la base, ahora tenemos que poner en marcha nuestras pruebas. Las pruebas nos arrojarán lo esperado en cuanto a eficacia, viabilidad y precisión a nivel general. Lo más importante serán los resultados de las pruebas, como forma de establecer que la organización está preparada para mantener el servicio estudiado, por eso deberán estar documentadas.
		SC:SG5.SP4	**Evaluar los resultados de las pruebas sobre el plan** Una vez hechos los test del plan de continuidad del servicio, revisaremos los resultados y los evaluaremos con el fin de encontrar mejoras y poder implantarlas. Lo esperado en estos casos es que los resultados del test sean los esperados de acuerdo a los objetivos definidos, y con la satisfacción del cumplimiento de los requisitos de entrada, pero no sucede así siempre. El producto de esta práctica serán el análisis documentado de los resultados, con los eventos no esperados y una lista de mejoras tanto al plan, y dependiendo de las circunstancias, al test.
	SC:SG6	**SC:SG6.SP1**	**Ejecutar planes** Una vez se definen los planes de continuidad del servicio y son probados, serán ejecutados y revisados. De manera inevitable los planes de continuidad del servicio se pondrán en marcha por diferentes razones. Lo que se espera es que se ejecuten como las condiciones lo requiere. Como buena práctica es que las condiciones se ejecuten en lo esperado y como lecciones aprendidas documentar la ejecución del plan.
		SC:SG6.SP2	**Medir la Efectividad del plan en operación** Después de la ejecución del plan, es necesario revisarlo post ejecución para identificar acciones correctivas que podrán ser implementadas como mejoras.
	SC:SG7	**SC:SG7.SP1**	**Establecer criterios de cambio** La ejecución real de los planes de continuidad del servicio nos dará condiciones reales en casos futuros, y aunque no es lo ideal, son lecciones aprendidas que serán aplicadas y que pueden mejorar y evitar consecuencias más graves. Por eso este proceso establece que los cambios a los planes de continuidad del servicio son identificados y gestionados. El producto de esta práctica son los criterios para hacer los cambios al plan de continuidad del servicio. Esto estará gestionado por los marcos de referencia que establezca la gestión de los cambios.
		SC:SG7.SP2	**Mantener los cambios a los planes** Al igual que se establecen los cambios, estos tienen que mantenerse bajo ciertas condiciones, y por los criterios que se establezcan. Por lo tanto de esta práctica se espera que sean las actualizaciones a los planes de continuidad y a la base de datos de los planes. Finalmente se buscará comunicar a la organización para que el personal esté al tanto de los cambios.
TM	**TM:SG1**	**TM:SG1.SP1**	**Priorizar los activos de tecnología** Hablar de software, para el Modelo CERT-RMM, es hablar de un activo de tipo tecnológico. La Gestión de TI que se establezca en la organización aportará en gran parte sobre todo a este proceso, teniendo en cuenta que manejará mejores prácticas para la gestión de activos de TI. Como se puede ver, la relación de las TI y los servicios pude llegar a ser significativa para la consecución de los objetivos que pone la compañía a nivel operacional. La priorización de estos activos tecnológicos es importante debido a que son recursos de gran importancia para la consecución de la misión de la organización por su soporte a la resiliencia operacional en cuanto a su contribución con los servicios. Toma importancia un activo, como el software, cuando se relaciona con activos de información, cuando lo provee un externo como servicio, si sirve para principios de redundancia, si aporta como control de la resiliencia de la organización o si hace parte de los planes que soportan la continuidad del servicio.

			Como resultado de esta práctica tenemos la lista de activos tecnológicos de alto valor (dentro del cual estará el software), que a su vez será suministrado por ADM y gestionado por nuestro marco de gestión de TI (Se sugiere COBIT), con esto podremos realizar de manera más eficaz la priorización y monitorización en caso de actualización
		TM:SG1.SP2	**Establecer los activos tecnológicos enfocados en la Resiliencia** Como se ha indicado, un software implementa resiliencia debido a la necesidad que tiene para la organización su funcionalidad en momentos de estrés o interrupción, pero esto quiere decir que posiblemente –y en su mayoría– soporta un servicio de alto valor para la organización –de los que estén en producción–, o ya sea que haga parte de los planes de restauración o ejecución de la continuidad del servicio. Esta práctica pretende que se identifiquen los activos de tecnología que soportan la continuidad del servicio y los planes de restauración. Con ayuda del marco de gestión de TI y el entorno de empresa que relaciona los servicios de alto valor, nos será fácil identificar los activos, y para nuestro caso el software que debe ser resiliente. Como producto de esta práctica tendremos la lista de los activos tecnológicos resilientes, y precisamente aquí se listará el software resiliente de la organización.
	TM:SG2	**TM:SG2.SP1**	**Asignar Requisitos de Resiliencia a los Activos de Tecnología** En esta práctica nos apoyaremos de lo definido en RRD, para establecer los requisitos de resiliencia a tener en cuenta por el activo, este será desde el punto de vista de gestión de la tecnología. ¿Por qué consideraremos en este paso estos requisitos?, esto es debido a que el software en sí mismo puede soportar o ser soportado por otro tipo de aplicaciones, con el fin de proteger y sostener el activo –una aplicación en sí misma puede protegerse con otra p. ej. Un sistema operativo puede necesitar de otra aplicación para su protección–. Es necesario identificar los conflictos de los requisitos y saberlos manejar. Finalmente tendremos documentados estos requisitos a tener en cuenta en el ciclo de vida del software que soporte los servicios
		TM:SG2.SP2	**Establecer e Implementar Controles** El sistema de control interno apoyará esta práctica, en cuanto a identificación e implementación de controles administrativos, técnicos y físicos que son requeridos para cumplir con los requisitos de resiliencia. Estos controles se implementarán con el fin de garantizar resiliencia operacional en los activos referentes a tecnología. Es claro que si se tiene una administración de la seguridad, como por ejemplo un SGSI basado en ISO 27001, y unos planes de continuidad, gran parte de los controles serán propuestos, pero los requisitos que nos proporcione RRD posiblemente nos harán implementar otros controles necesarios. Este punto es una motivación para establecer medidas dependiendo del tipo de software debido a que dentro de estos controles es importante establecerlos durante el diseño, construcción y adquisición como tal del software. Como producto de esta práctica tenemos identificados e implementaremos los controles administrativos (p. ej. Políticas a usuarios y de uso, Estándares de Interoperabilidad, procedimientos sobre personal…), técnicos (p. ej. Gestión del cambio y configuración, Aseguramiento de calidad de software, auditoría de software de grano fino,…) y físicos (aunque en el software será mucho más de soporte físico de operación) necesarios.
	TM:SG3	**TM:SG3.SP1**	**Identificar y evaluar los riesgos de activos de tecnología** Los activos tecnológicos estarán expuestos a riesgos, y el software igual, por esto se tendrá que identificar y evaluar los riesgos que le afectan. Esta práctica será conducida por los elementos que nos proporcione el marco de gestión de riesgos y las prácticas en RISK. Con esto podemos listar los riesgos que afectan a estos activos, en este caso el software (p.ej. riesgos de acciones intencionadas y no intencionadas que comprometen la protección, pobre implementación de controles que aseguren continuidad, pobre diseño y proceso de construcción…) y su impacto para la organización, esto se hará bajo criterios establecidos, de modo que con base a esto se establezca la categorización y priorización de los mismos.
		TM:SG3.SP2	**Mitigar los Riesgos Tecnológicos** Una vez identificados los riesgos a los que se ven comprometidos los activos de tecnología, es necesario establecer las medidas e implementarlas de acuerdo a la estrategia de la compañía. La idea es que el riesgo se encuentre en los niveles establecidos, y que se mitigue si se materializa a través de estrategias de protección que asegurarán el manejo del riesgo y la recuperación del activo sobre las consecuencias del impacto. Como resultado de esta práctica tendremos unos planes de mitigación junto a la lista de los responsables que van a conducir las estrategias de mitigación. Esto será monitorizado para posteriormente manejar el riesgo residual. De igual manera será soportado por el proceso RISK.
	TM:SG4	**TM:SG4.SP1**	**Controlar el acceso a los activos de tecnología** Para asegurarse que los activos de tecnología, y para nuestro caso el software, funcione de manera apropiada y con los resultados esperados es necesario gestionar su Integridad. El primer objetivo es asegurarse que el software no sea modificado, esto incluye la modificación no autorizada de código de software, sistemas, aplicaciones,

			sistemas operativos, herramientas y otros activos tecnológicos basados en software. La gestión de TI que implementa mejores prácticas, como COBIT –para la gestión de los activos de tecnología –, ISO 20000 o ITIL –para gestión de la configuración, gestión del cambio y gestión de la entrega–, e ISO 27001 –para controlar la seguridad (Triada CID)– podrán tener una ventaja competitiva para garantizar esto. El primer paso es controlar el acceso, esto quiere decir que existan medidas que controlen el acceso sólo a personal autorizado, y aseguren que no se hagan modificaciones conscientes e inconscientes del software. Estas medidas para el software suelen ser tecnológicas, a diferencia del hardware que implementa tanto medidas electrónicas como físicas. Hay que considerar los procedimientos que requerirán control de acceso, como modificaciones o actualizaciones, mantenimientos, conexiones a bases de datos, etc. Como producto de esta práctica tendremos que plantear políticas y procedimientos para el acceso (p.ej. Políticas para la gestión de acceso, Procesos de autorización de acceso, roles de usuario, políticas de gestión de identidades,…), implementar listas de control de acceso y herramientas necesarias de apoyo, así como una lista de miembros autorizados en la modificación del activo (relacionado con la gestión del cambio), en nuestro caso el software, logs y registros de auditoría.
		TM:SG4.SP2	**Ejecutar la gestión de la configuración** Uno de los aspectos contemplados dentro de la gestión de TI es la gestión de la configuración. Dentro de la resiliencia soporta la integridad de los activos de tecnología asegurando que pueden ser restaurados a un estado aceptable cuando sea necesario y provee un nivel de control sobre los cambios que afectan los servicios de la organización. La gestión de los servicios de TI establece los ítems de configuración, que son los elementos a gestionar, y para los cuales se realiza una gestión durante todo el ciclo de vida, desde sus fases de desarrollo, hasta su operación y mantenimiento, estableciendo controles durante su servicio. Se debe tener una atención especial con el software debido a que requieren estrictos niveles de control de la configuración, debido a la cantidad de cambios que se le realizan. El producto de esta práctica serán los procedimientos, políticas, directrices, normas y cuantos elementos crea la organización para gestionar la configuración de los activos de tecnología esto aplica tanto si el software es construido e implementado, usado o adquirido, tanto de manera interna como externa. Se sugiere el uso de ISO 20000 o ITIL, que implicará tenerlos en la Base de datos de configuración CMDB debidamente identificados y controlados –a través de logs y reportes–. Del mismo modo en esta práctica se propondrá las herramientas, técnicas y métodos que soportarán la gestión de la configuración. Esto a su vez podrá ser auditado. También se puede considerar unos planes de acción. Esta práctica será controlada por la gestión del cambio TM:SG4.SP3.
		TM:SG4.SP3	**Ejecutar la gestión y control del cambio** El software tiende a tener un comportamiento complejo debido a los modelos de madurez, los ciclos de desarrollo iterativos, requisitos emergentes, mejora de funcionalidades y demás, que lo hará estar en constante cambio durante su ciclo de vida, por lo tanto será trascendente que se gestionen los cambios. Los cambios tienen un papel importante en el software, por lo tanto tendrán que gestionarse para evaluar su impacto, ya sea económico, en el servicio que soporta, con otros activos que soporten servicios, etc. Del mismo modo, los cambios aportarán no solo a las mejoras, sino a la detección de fallos y mantenimiento, por eso una buena gestión garantiza un buen manejo alineado con los requisitos de la organización en cuanto a resiliencia. Como producto de esta práctica tenemos los puntos de referencia para suministrar a la gestión de configuración TM:SG4.SP2, pues la gestión del cambio se encarga de administrar los cambios a los elementos de configuración. Además establecerá las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para establecer los cambios, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, a las peticiones de cambio que se realicen se les debe hacer un respectivo seguimiento, el cual se almacenará en la base de datos de gestión del cambio.
		TM:SG4.SP4	**Ejecutar la gestión de la entrega** Para la gestión de servicios de TI, es necesario, del mismo modo como se establece la gestión de la configuración y del cambio, gestionar la entrega del activo tecnológico al entorno de producción. Para la gestión de la entrega en software es importante tener en cuenta el manejo de versiones, pero así mismo estas deben ser probadas antes de salir a producción y durante producción. En tecnología se maneja el término *Build* como una versión del activo que está listo para ser entregado en producción, en el caso del software puede ser por ejemplo una versión actualizada de un sistema de gestión que incorpora una mejora de seguridad. La entrega de los *builds* debe ser probada en un entorno para identificar situaciones que puedan comprometer otros activos, que refleje problemas de seguridad, etc. Una vez se identifique y se realicen las mejoras esperadas, de establecerá la entrega en producción. Así mismo en este proceso, los parches (que aportarán a la resiliencia en cuanto a mejorar el software en cuanto a gestión de vulnerabilidades) serán un tipo de entrega y tendrá que ser gestionado. Como producto de esta práctica se establecerán las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para la gestión de la entrega, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, se recomienda la entrega de *Builds*, pero del mismo modo se debe establecer un plan y procedimiento para probar las entregas, documentar los resultados de las pruebas a los *Builds*, establecer las mejoras y entregar a producción. La

			gestión de la entrega estará relacionada con los procesos de gestión de la configuración y del cambio.
	TM:SG5	TM:SG5.SP1	**Ejecutar la planeación para el sostenimiento de activos de tecnología** Así como se gestiona la integridad, para los activos de tecnología que soportan servicios, o que son de alto valor tienen que asegurar su disponibilidad y funcionalidad, por lo tanto deben desarrollarse planes que ayuden a su sostenimiento. Los requisitos de resiliencia establecidos, definirán ciertos términos en cuanto a disponibilidad que se deben cumplir, tanto en condiciones del día a día, como en el caso que se presente una situación de interrupción o estrés. Para esto se definen una serie de las métricas que permitan establecer la disponibilidad que debe cumplir la tecnología y servicios relacionados, tanto en condiciones normales como en condiciones degradadas. En este proceso, para cada activo se establece el *Recovery time objectives* (RTOs), que consiste en el periodo aceptable de baja de un activo tecnológico y su servicio asociado, después de que la organización se ve comprometida por una situación que impacta su operación normal, este será incluido en los planes de continuidad (Área de Proceso SC) debido a que está ligado al servicio. También se establece un *Recovery point objectives* (RPOs) en el cual se define el punto en el cuál un activo tecnológico debe ser restaurado para permitir la recuperación de los activos y servicios asociados después de la interrupción, este será incluido en los planes de continuidad (Área de Proceso SC) en cuanto a la restauración. Como producto de esta práctica se tendrá como referente los resultados del análisis de impacto en el negocio o la evaluación de riesgos (Área de Proceso RISK) con el fin de definir el alcance de sostenimiento de los activos. Igualmente se deben definir las métricas (Esto se definirá en RRD y RRM). También de recogerán los RTOs y los RPOs y esto se tendrá en cuenta en los planes de continuidad del servicio (Área de Proceso SC).
		TM:SG5.SP2	**Gestionar el mantenimiento de los activos de tecnología** Es claro que tendremos que establecer una práctica en la que se definan y se gestionen los mantenimientos operativos de los activos de tecnología. Tal vez esto suene mucho más para el hardware, sin embargo el ciclo de vida del software contempla el mantenimiento con el fin de mejorar el software, por ejemplo la aplicación de parches para corregir una vulnerabilidad u optimizar un algoritmo (gestionado por TM:SG4.SP4.). El riesgo de este tipo de mantenimiento, es una posible acción, intencionada o no, que podrá terminar comprometiendo los requisitos de resiliencia establecidos. Por esta razón, este tipo de mantenimiento necesita procedimientos de control, autorización y acceso. Como producto de esta práctica tenemos la lista de mantenimiento regular que requieren los activos de tecnología junto con intervalo y especificaciones, aunque en el caso del software consistiría en lo que se pacte de mantenimiento en el contrato de adquisición. Se deberá establecer una lista de personal autorizado para realizar las reparaciones. Se tendrá un documento de seguimiento con los mantenimientos registrados (tanto correctivo, preventivo, adaptativo o perfectivo). Se tendrán registradas las peticiones de mantenimiento. Esto deberá alinearse y estar controlado con la práctica que establece la gestión de cambios. En el caso de software es importante tener en cuenta la norma ISO/IEC 14764.
		TM:SG5.SP3	**Gestionar la capacidad de la tecnología** La gestión del servicio de TI, establece otra gestión que se debe hacer dentro de los activos de TI, y es la gestión de la capacidad. Para efectos de la guía, es importante tener en cuenta la capacidad operativa de los activos y poderla gestionar de manera adecuada esto debido a que la capacidad es una propiedad que está directamente relacionada a la disponibilidad. La planeación de la capacidad debe hacer previsiones, debido a la variabilidad que tiene la demanda del servicio (p.ej. horas pico y horas valle del servicio). En cuanto a software, la capacidad puede relacionarse con varias situaciones, por ejemplo usuarios concurrentes en una aplicación, la cantidad de peticiones que recibe, cantidad de espacio en memoria que utiliza, etc. El producto de esta práctica será el establecimiento de una estrategia que defina la gestión de la capacidad. Para construcción de software es importante que se defina en los requisitos de manera clara de la capacidad necesaria para el funcionamiento bajo cualquier condición. Adicionalmente se tendrá en cuenta marcos de referencia como ITIL e ISO 20000 para la gestión de la capacidad. Es recomendable hacer estimaciones y previsiones de las condiciones que cumplirá el software en cuanto a capacidad, por lo tanto es importante documentar los requisitos (previstos por RRD), y todos los procedimientos, políticas, planes, para su aseguramiento (esto puede afectar RPO y RTO). Para conocer el rendimiento de la estrategia, es importante establecer unas métricas para poder establecer planes de acción, y estos planes estarán ligados a los procesos de gestión de cambio.
		TM:SG5.SP4	**Gestionar la interoperabilidad de la tecnología** Actualmente la interoperabilidad de aplicaciones es un factor importante que se maneja en la organización, esto debido a las estructuras emergentes, virtualización e interconexión entre las empresas, y en general entre los sistemas. En el software específicamente se describe como la capacidad de diferentes aplicaciones de intercambiar los datos a través de formatos comunes, para entenderse en el mismo lenguaje. La importancia de gestionar la interoperabilidad es que es al día de hoy un importante factor que representa valor para la organización

			Como producto de esta práctica se establecerán los estándares seguidos para la interoperabilidad de modo que la arquitectura y diseño de la aplicación se basen en esos principios y mantengan el valor en cuanto a interoperabilidad minimizando los riesgos que esto implica (considerados por RISK). Se sugiere el uso de estándares para tener en cuenta en aspectos de diseño, desarrollo e implementación de arquitecturas interoperables, integración apropiada de sistemas (construidos, adquiridos o contratados), diseño adecuado de interfaces, manejo de "sistemas de sistemas", etc.

Tabla 19. Mapa de ruta para Software adquirido basado en áreas de proceso CERT-RMM

5.1.4 Software como servicio contratado

Área de Proceso	Metas	Prácticas	Recomendaciones
ADM	**ADM:SG1**	**ADM:SG1.SP1**	**Inventario de Activos** Es importante para la organización mantener de manera organizada sus activos, y del mismo modo se espera que la organización siga unas mejores prácticas en cuanto a la gestión de los mismos. Debido a que tratamos con software se debe tener en cuenta que al ser un activo intangible relacionado con tecnología, no tendrá un manejo igual al que tendrá un activo físico. De esta manera la gestión de TI debe asegure de establecer una adecuada gestión de activos de TI para asegurar que los sistemas software e infraestructuras permanecen eficaces, eficientes y son aceptables y se retiran de servicio de manera adecuada y/o se reemplazan cuando no cumplen dichos criterios, todo esto alineado con el marco de gobernanza de TI. En el caso del software como servicio contratado, moverse al Cloud exime la responsabilidad en el funcionamiento y el soporte de las aplicaciones, pero implica un especial cuidado de los SLA y los contratos referentes a la prestación del servicio, siendo este directamente un activo de servicio. Un concepto importante es *Software Asset Management* (SAM), que corresponde a que a nivel de negocio se realice una adecuada gestión de la adquisición, mantenimiento, uso y disposición de las aplicaciones software dentro de la organización y la optimización de los procesos que se gestionan. Se sugiere utilizar marcos de gestión de software como ISO/IEC 19770 que se complementa con ISO 20000 en el proceso Gestión de la Configuración y en la cual la organización puede demostrar que realiza una gestión de activos de software. De igual manera ITILv3 incluye el proceso de Activos de Servicio y Gestión de la Configuración. COBIT 5 está alineado con ITILv3, por lo tanto puede considerar el inventario a alto nivel en la gestión de TI. Del mismo modo, SAM aporta a ISO/IEC 27002, en lo que a incidentes de seguridad de Software considera, es por esto que será un control preventivo a situaciones de interrupción o estrés. El producto de esta práctica debe ser un inventario y una base de datos del software de la organización. Del mismo modo se deberá identificar cuál software que se produce soporta procesos críticos del negocio y son vitales para la operación y la consecución de los objetivos de la organización. Se establecerá el valor de cada software que se produzca.
		ADM:SG1.SP2	**Establecer un Entendimiento Común** Es importante que se clasifiquen los activos software dentro de los activos de tecnología, del mismo modo, usando uno de los marcos sugeridos en ADM:SG1.SP1 se tendrá una buena práctica para que se manejen los activos de manera adecuada, y podrá ser el punto de partida para que se puedan asignar tanto a propietarios como vigilantes y entiendan sus responsabilidades (en la siguiente práctica ADM:SG1.SP3). El entendimiento será un punto de partida para evaluar las prioridades sobre los activos software en cuanto a resiliencia operacional, para saber cuáles tienen mayor valor para la organización en cuanto a resiliencia operacional no solo porque sean activos de alto valor sino también por los servicios que soporten, cuáles soportan servicios críticos y a partir de esto dará un enfoque global para establecer los requisitos de resiliencia. En este escenario, la organización contratada y contratante tendrán que dejar en claro en el *Service Level Agreement* SLA, cuáles son las responsabilidades sobre el servicio de cada parte... A través de esta práctica se llegará al entendimiento mutuo de los activos software y sobre todo cuáles son los de mayor importancia por soportar los servicios de la organización. Esto se puede realizar documentando la información necesaria, como políticas de uso, importancia y concienciación del activo frente a los servicios, entre

			otros.
		ADM:SG1.SP3	**Establecer Propietarios y Vigilantes** El software, como el resto de activos, tendrá asociados unos propietarios y unos vigilantes. Establecer mejores prácticas ADM:SG1.SP1 en general sobre los activos, y con un entendimiento común ADM:SG1.SP2 del aporte del software a la organización hará mucho más fácil establecer quién es quién dentro de las funciones del activo, y del mismo modo establecerá las pautas para la resiliencia operacional de la organización. Por un lado se establecerán los propietarios que tendrán la responsabilidad de la viabilidad, productividad y resiliencia del software, no necesariamente serán personas directamente, pueden ser unidades organizacionales internas o externas, dependiendo lo que se defina en el SLA. Por otro lado se establecerán vigilantes –que también serán personas o unidades organizacionales internas o externas– con la responsabilidad de implementar y gestionar los controles para satisfacer los requisitos de resiliencia, mientras estén a cargo del activo. Cabe resaltar que como se indicó anteriormente, en todos los casos, los propietarios son los responsables de asegurar la protección y continuidad apropiada de sus activos, sin tener en cuenta las acciones (o inacciones) de los vigilantes. El resultado de esta práctica será la identificación de los propietarios y los vigilantes y la actualización de los perfiles y las bases de datos de activos definidos. Es importante definir el perfil de propietario y vigilante y las responsabilidades que tienen con el software. En caso que el software soporte junto a un grupo de activos un servicio de la organización, es necesario establecer este grupo dentro de la identificación.
	ADM:SG2	**ADM:SG2.SP1**	**Asociar Activos con Servicios** Una práctica muy importante es empezar a establecer la relación de los activos con los servicios de la organización. Para una organización, asociar activos con los servicios es una práctica muy significativa debido a que es mucho más importante establecer resiliencia en un servicio de alto valor, que en un servicio complementario. La resiliencia operacional busca que la organización se enfoque en la visión de los servicios, debido a esto asociará el activo al servicio que soporta. En el caso del SaaS, es claro que la organización debió pasar por un proceso de adquisición y se tendrá claro cuáles servicios van a asociarse y cuál será su rol para soportar el servicio. A partir de esta definición, será más fácil establecer las mejores estrategias en cuanto a protección y sostenimiento del software. Como resultado de esta práctica tendremos qué software se relaciona a los servicios de alto valor de la organización.
		ADM:SG2.SP2	**Analizar dependencias entre activos y servicios** Un activo puede soportar uno o más servicios, por esto se debe realizar un análisis general de estos servicios en la organización. Un CRM por ejemplo puede soportar varios servicios de la organización, y del funcionamiento de este podrán verse afectados uno o más servicios de alto valor. Una buena identificación de las dependencias es crucial pues será base para el establecimiento de los requisitos de resiliencia y por ende la estrategia de protección y sostenimiento del software. Como resultado de esta práctica evitaremos los conflictos potenciales por dependencias entre activos y se establecerán acciones y soluciones de mitigación.
	ADM:SG3	**ADM:SG3.SP1**	**Identificar Criterios de Cambios** (Esta práctica será complementaria a RRM:SG1.SP3) El ajuste a las necesidades de la organización y específicamente a los requisitos de resiliencia, afectará de manera directa al activo o a la asociación que tenga con un servicio, es por esto que se debe tener una práctica que sirva de soporte para el establecimiento y mantenimiento de los cambios. Los cambios identificados pueden afectar a uno o más activos, por esto las prácticas anteriores deberán soportar la estrategia de gestión del cambio establecida por la organización. Para este caso, es común que frente a otras estrategias, haya un especial cuidado de gestión del cambio en el SaaS, debido a que la organización escoge una solución cloud con la ventaja de ajustar el software cuando lo necesite, por lo tanto el énfasis se hará en el servicio como tal. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se 0resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
		ADM:SG3.SP2	**Mantener Cambios a los Activos e Inventarios** (Esta práctica será complementaria a RRM:SG1.SP3) Así como se identifican los cambios, es necesario gestionarlos de manera adecuada, teniendo en cuenta los marcos de referencia que utilice la organización para el mantenimiento de cambios. Como se indicó en la práctica anterior, las soluciones Cloud son cambiantes, por lo tanto se hará un mayor énfasis en el seguimiento, pero también en lo que se establezca en el SLA. El proveedor Cloud deberá ofrecer las garantías en la documentación y seguimiento de los cambios, sobre todo cuando la mayoría de la

			responsabilidad estará en juego. Por esta razón es importante cerciorarse la estrategia de gestión del cambio que sigue el proveedor cloud. Esta práctica pretende que haya procedimientos documentados de la gestión de cambios en el activo y que se tenga presente el estado del activo en ciertos instantes, de acorde a esto establecer los requisitos de resiliencia y la estrategia de protección y sostenimiento del software y de los servicios que soportan. Es recomendable mantener esta práctica con los procesos de gestión del cambio, en esto se resalta la importancia y el valor que le da a la organización alinear ISO 20000 o ITIL junto con sus procesos para la gestión de activos, y en este caso la gestión del software.
EXD	**EXD:SG1**	**EXD:SG1.SP1**	**Identificar Dependencias externas** Este proceso es muy importante para este tipo de software. Cuando un tercero participa dentro de los procesos de la organización, la complejidad de las relaciones de la organización y los escenarios de riesgo aumentan. En este caso, construir, mantener o contratar software por un tercero. Estos terceros se considerarán dependencias externas, pues el activo –y el servicio– estará sujeto a las acciones de la entidad. Estas entidades tendrán que identificarse y priorizarse para asegurar la resiliencia de los servicios de alto valor que soportan, por lo tanto se identificará para entender, formalizar, monitorizar y gestionar los riesgos que esto ocasiona. Del mismo modo tener claro si soportan parte o todo un servicio y saber de qué activos son propietarios. Es importante recopilar toda la información, contratos entre proveedores, SLA, entre otros. El resultado de esta práctica será una lista detallada de las diferentes dependencias externas (descripción, activos y servicios que soportan, contratos,…), y un procedimiento documentado para la actualización de las mismas.
		EXD:SG1.SP2	**Priorizar dependencias externas** Es importante establecer prioridades sobre las entidades externas dependiendo de la importancia que tenga en la entrega de servicios de alto valor. Es importante realizar la priorización de dependencias externas pues la organización delega ciertas responsabilidades sobre los requisitos de resiliencia a dichas dependencias que manejan ciertos servicios, lo que le implica un papel importante para la consecución de la misión de la organización. El producto de esta práctica es establecer los criterios para priorizar estas entidades externas, y a partir de estos criterios se realizará la priorización de las dependencias externas, y los análisis de afinidad de las dependencias externas.
	EXD:SG2	**EXD:SG2.SP2**	**Identificar y evaluar riesgos debido a dependencias externas** Como se decía anteriormente, contratar una entidad externa aumenta la complejidad de las relaciones de la organización, pero también su entorno de riesgos. La gestión de riesgos de la organización juega un papel importante pues tiene que entender esa complejidad y ajustar la gestión a un número considerable de nuevos riesgos. Este proceso indica que se deben identificar y evaluar esos riesgos que se asumen al contratar a un tercero. Debido a que esto está involucrado en la gestión de riesgos se manejará en las prácticas RISK:SG3 y RISK:SG4. Por lo tanto el producto de esta práctica será las declaraciones de riesgos de dependencias externas con la evaluación de impacto y la lista de riesgos de las dependencias externas con categorización y priorización.
		EXD:SG2.SP2	**Mitigar riesgos debido a dependencias externas** La gestión de riesgos de la organización, entendiendo el nuevo escenario de riesgos que se crea, debe establecer e implementar las estrategias de mitigación, con el fin de mantener en un nivel aceptable de los riesgos derivados de las relaciones con dependencias externas. El producto de esta práctica serán los planes de mitigación de los riesgos de dependencias externas –donde se considera el desarrollo y revisión de controles– y la implementación y monitorización de la efectividad de los planes. Del mismo modo las prácticas serán complementadas por el proceso RISK:SG5.
	EXD:SG3	**EXD:SG3.SP1**	**Establecer especificaciones empresariales para dependencias externas** En general las relaciones con las entidades externas tienen que ser de tipo formal, a través de contratos o acuerdos que contribuyan seguridad al gobierno de la organización. Para escoger los proveedores, es necesario que estos demuestren que pueden cumplir lo que requiere la organización y que se ajustarán a las especificaciones del contrato. Al soportar servicios de la organización, las entidades externas se convierten en una extensión de la organización y la organización debe hacer que las entidades externas sean conscientes de la importancia de las políticas, estándares, lineamientos internos que a la larga son controles que ayudan a proteger y sostener las operación de la organización, siendo esto un apoyo para la resiliencia de la organización. Este pacto debe acordarse a nivel de empresa de modo que haya ese compromiso con la estrategia de resiliencia de la organización.

			Por esto a los externos se les compartirá los requisitos de resiliencia para que los tengan en cuenta RRD, y especificaciones referentes a los requisitos del software como tal (Por ejemplo, que el software se ajuste a los lineamientos establecidos por el Área de proceso RTSE, pues aunque no lo hace directamente se debe acordar que hayan prácticas como las ahí citadas). Como producto tendremos la lista de especificaciones de empresa que aplican a dependencias y entidades externas y las plantillas de acuerdo que reflejan las especificaciones empresariales.
		EXD:SG3.SP2	**Establecer especificaciones de resiliencia para dependencias externas** Así como a nivel de empresa se realiza este acuerdo, es necesario que se dejen claras las especificaciones de resiliencia que aplican para las entidades y dependencias externas. Una dependencia externa es el resultado del acceso de una entidad externa para controlar, desarrollar, poseer, ser responsable (de operación, mantenimiento o soporte), o tener obligaciones definidas relacionadas con uno o más activos o servicios de alto valor para la organización. Esos servicios tendrán unos requisitos de resiliencia y por ende la entidad externa tendrá un compromiso con el alcance de esos requisitos. Como producto de esta práctica se tendrán las especificaciones de resiliencia documentada y el acuerdo de nivel de servicio SLA. Es importante establecer comportamientos requeridos y normas de rendimiento esperados (disponibilidad, rendimiento, gestión del cambio, seguridad, continuidad del negocio…) con el fin de medir que se cumpla con los requisitos específicos
		EXD:SG3.SP3	**Evaluar y seleccionar entidades externas** Como se ha indicado, el proceso de elección de un tercero para realizar un proceso como en este caso construir/mantener/implantar/ofrecer software, debe ser estricto y tener como referencia unas especificaciones claves y unos criterios de selección adecuados. Las entidades externas son seleccionadas basadas en una evaluación de su habilidad de cumplir con las especificaciones establecidas en EXD:SG3.SP1 y EXD:SG3.SP2. Es decir, adicional al proceso de contrato, deberá tenerse en cuenta cumplir con las expectativas de resiliencia necesarias Como producto de estas prácticas se deberá establecer un proceso de selección que incluya los requisitos esperados (preferiblemente a través de documentos que comprueben la capacidad de cumplimiento), establecer criterios de selección, evaluar las propuestas frente a los criterios y tomar una decisión.
		EXD:SG3.SP4	**Formalizar relaciones** Una vez tomada la decisión, lo que queda es establecer y mantener un acuerdo formal con la organización que ofrece las mejores condiciones de servicio y que cumple con las expectativas de la organización. El acuerdo dependerá del servicio o producto que se contrate, dependerá de la relación entre las entidades, los niveles de integración. Como producto de esta práctica tendremos el acuerdo con la entidad externa. En este acuerdo deberán estar cuestiones documentales como términos, condiciones, especificaciones, entre otros, al igual que permisos, licencias y demás. Deberá incluir también los manejos de desarrollo del trabajo, especificaciones, estándares de desarrollo y prácticas a utilizar para mantener el servicio, seguridad, gestión de riesgos, estrategias de protección y sostenimiento de producto y proceso, … Y cuanta documentación y aclaración necesite estar documentada orientado a tener los términos del servicio claro.
	EXD:SG4	**EXD:SG4.SP1**	**Monitorear rendimiento de entidades externas** Para saber el rendimiento de la entidad externa la mejor manera es monitorizando su actividad y esto lo hará de acuerdo a las especificaciones establecidas, estas serán el resultado de EXD:SG3. Esto se hará de manera periódica para tener un registro y en ciertos casos tomar decisiones. Algunos criterios de medición serán los que se establezca en el acuerdo formal. En algunos casos, los cambios que se hagan y las decisiones también dependerá del ambiente cambiante de riesgos. Como producto de esta práctica tenemos los reportes de las entidades externas, las bases de datos de gestión de relaciones que nos muestra la información de la monitorización del rendimiento actual, y reportes de inspección de entregas de la entidad externa. La monitorización deberá ser un procedimiento conocido y con responsables.
		EXD:SG4.SP2	**Corregir rendimiento de entidades externas** Dependiendo de los resultados monitorización realizada, se llevarán a cabo acciones correctivas para apoyar el rendimiento de la entidad externa, esto es muy importante en un ciclo de mejora continua. Entre menos dependa de externos la continuidad de los servicios, mejor. Las acciones correctivas estarán en el acuerdo. Como productos de esta sección tenemos los reportes o documentación de acciones correctivas, estas se evalúan y se escogen las mejores acciones correctivas entre las alternativas propuestas, y se realiza una documentación con las acciones correctivas escogidas. Esto debe comunicarse a la entidad externa. Como es mejora continua

			vendrá la implementación, monitorización y actualización en caso que se requiera.
RISK	**RISK:SG1**	**RISK:SG1.SP1**	**Determinar las categorías y fuentes de Riesgo** Es necesario que se establezcan las fuentes de riesgo a las que se va a exponer el software, no solo como producto sino como proceso, y a partir de esto establecer las categorías y una taxonomía del riesgo operacional, que es el que implica directamente la operación habitual de los servicios. Identificar el riesgo es comprender a qué se enfrentará el software, y a pesar de no poder contar con todos los escenarios posibles ni blindar la operación a todas las amenazas, lo más importante es identificar lo más crítico y considerar los *Black Swan.* Hay que considerar las fuentes tanto internas como externas. La organización debe establecer un marco para la gestión de riesgos que tenga una visión holística del software, como se indicó en el Capítulo 2 seguir un estándar como ISO 31000 junto con mejores prácticas para el ciclo de vida del software (no solo del producto sino del proceso) nos ayudará a establecer lo que se espera de esta práctica, el riesgo operacional al que se expone el software, las categorías de riesgo y la taxonomía. Este marco de referencia será el apoyo para la definición de los requisitos de resiliencia.
		RISK:SG1.SP2	**Establecer una estrategia para la Gestión de Riesgo Operacional** La organización que cuenta con un marco para la gestión del riesgo empresarial ERM, generalmente cuenta con la base necesaria para establecer la gestión de riesgo operacional ORM. De acuerdo como decida la organización su estrategia a nivel ejecutivo, decidirá cuál será la estrategia a seguir para la ORM que cumpla con los objetivos del negocio. La estrategia que se establezca será la que defina el desarrollo de las actividades relacionadas con la ORM y la colección, coordinación y gestión de dichos riesgos al marco de procesos de ERM. Dentro de la estrategia se debe contar con que el software contratará como servicio, por tanto se considerará que el mantenimiento del software será responsabilidad de terceros, por lo tanto aumentará la complejidad de los escenarios de riesgos y del mismo modo habrá una delegación de responsabilidades en la gestión de riesgos. La estrategia debe estar documentada y comunicada a todos los interesados internos y externos responsables de las actividades de ORM, de modo que se tenga el entendimiento y sirva de entrada para otros procesos –por ejemplo para definir los requisitos de resiliencia.
	RISK:SG2	**RISK:SG2.SP1**	**Definir los parámetros de Riesgo** Para evaluar la relevancia del riesgo operacional en la organización, es preciso establecer unos parámetros con los cuales se pueda medir, es decir, se tenga una fotografía del estado actual de la organización. Para esto se definirán unos umbrales de tolerancia de riesgo que reflejará el nivel de riesgo dispuesto a admitir y a enfrentar la organización. Este deberá considerar que el riesgo implicará el producto y el servicio directamente, la gestión deberá considerar lo que contrata con el tercero. Con un marco de gestión de riesgos, es claro que se establecerán estas medidas, y que acorde a la estrategia y objetivos de la organización se dictarán los parámetros a los que quiere apuntar y con los que evaluará el riesgo operacional, y con los cuáles definirá los requisitos para la gestión de riesgos.
		RISK:SG2.SP2	**Establecer criterios de medida del riesgo** Así como se definen los parámetros, es necesario definir los criterios para medir el impacto del riesgo dentro de la organización. Estos criterios serán importantes para clasificar, evaluar y priorizar los riesgos operacionales. El producto de esta práctica es el conocimiento de las áreas de impacto –donde el riesgo material tiene consecuencias significativas e interruptivas– priorización de dichas áreas y un documento con los criterios de medida y evaluación y con la probabilidad de riesgos.
	RISK:SG3	**RISK:SG3.SP1**	**Identificar los Niveles de riesgo en los Activos** Antes de establecer resiliencia operacional sobre los activos, es preciso que se tenga claro que los activos y por ende servicios se pueden ver afectados por los riesgos operacionales, por lo tanto su identificación y mitigación es primordial. Acorde a las categorías y al nivel de riesgo definidos por la organización, se identificarán los riesgos que afecten a los activos, en este caso al software. Eso sí, es claro que no se identificará la totalidad de riesgos, pero al menos los riesgos operacionales que afecten los servicios, estos deben ser identificados y gestionados a través de diferentes técnicas. De ahí la importancia de seguir uno de los marcos para la gestión de riesgos. Deberá considerarse los escenarios en los cuales la gestión sea por parte de la organización, y pactar en el SLA los escenarios en los que sea parte del tercero. Como producto de esta práctica, tendremos un conjunto de herramientas para la identificación del riesgo organizacional, y una lista de riesgos categorizados por activo.

		RISK:SG3.SP2	**Identificar los Niveles de riesgo en los Servicios** El objeto de establecer la resiliencia operacional, es garantizar que los servicios cumplan la misión, sin embargo estos servicios están expuestos a unos riesgos operacionales que son el resultado de una serie de riesgos sobre los activos de la organización. Por esta razón hay que evaluarse el impacto potencial de un riesgo sobre un activo, en este caso los riesgos sobre el funcionamiento del software, y su impacto sobre la misión del servicio. De acuerdo a esto no solo se puede mitigar sino priorizar teniendo en cuenta los intereses de la organización. Se asume que la organización identificó de manera esencial los servicios de alto valor, y en el proceso ADM los activos asociados a estos servicios. Como resultado de esto podremos clasificar los riesgos por servicio y establecer contextos donde afecta el servicio y consecuencias de los riesgos sobre los servicios si se llegan a materializar.
	RISK:SG4	**RISK:SG4.SP1**	**Evaluar Riesgos** Teniendo como lineamiento las prácticas realizadas anteriormente para la medición del riesgo (tolerancia, criterios e impactos del riesgo), lo siguiente es evaluar el riesgo operacional y sus consecuencias. Los riesgos varían en cada caso y específicamente para el software tenemos que considerar los diversos escenarios a los cuales esté expuesto el proceso. Esta evaluación nos dará una idea de cómo manejaremos el impacto de los riesgos y cómo actuar en diversas circunstancias operativas. El producto de esta práctica será la evaluación con base a los lineamientos de la organización y darle un valor cualitativo para poder decidir cómo actuar, y cómo priorizarlos.
		RISK:SG4.SP2	**Categorizar y Priorizar Riesgos** Una vez evaluados, podemos categorizar los riesgos operacionales de modo que establezcamos las prioridades sobre las actuaciones que se vayan a realizar sobre los mismos. Las categorías dependerán de los intereses, pero hay diferentes maneras de categorizas, por fuentes, por nivel de riesgo, por taxonomía, etc. Es importante tener en cuenta los escenarios y no olvidar los *Black Swan*, que en muchos casos son causas drásticas de interrupción o estrés del servicio. La priorización será importante a la hora de establecer resiliencia. Como resultado de esta práctica tendremos los riesgos por categorías y con priorización, de acuerdo a los intereses de la organización.
		RISK:SG4.SP3	**Asignar disposición al Riesgo** Del mismo modo que la organización asume que hay entendimiento de los riesgos, puesto que de acuerdo a su postura se evalúa, tiene también que documentar y aprobar su posición frente a los escenarios de riesgo identificados. Las acciones que tome de acuerdo a los riesgos tendrán que ser el producto de la estrategia establecida en la gestión de riesgos. La organización puede tomar diferentes disposiciones, entre ellas evitar el riesgo, aceptar el riesgo, transferir el riesgo o mitigar y controlar. Como producto de esta práctica de deberá listar los riesgos y la disposición de la organización, y los riesgos priorizados para mitigar. La disposición al riesgo será documentada y debidamente aprobada por la organización (en especial con los riesgos que se aceptarán).
	RISK:SG5	**RISK:SG5.SP1**	**Desarrollar planes para la mitigación del riesgo** Es necesario que se desarrollen planes de mitigación, sobre todo cuando el riesgo, producto de la evaluación realizada, está sobre el umbral y es inaceptable de admitir, no se desea transferir, y evitar solo sea posible eliminando la actividad que lo genera. La mitigación del riesgo puede requerir actividades referentes a la protección y sostenimiento del activo, o en algunos casos implementación de controles. En algunos casos las actividades no son suficientes y se deberá considerar el riesgo residual. Como práctica resultante tendremos el plan de mitigación del riesgo, para todos los riesgos a los que se dispuso mitigar y controlar. En este plan debe estar claro cómo se reduce la amenaza o cómo se protege la vulnerabilidad, las acciones preventivas, los controles a implementar, los planes de continuidad del servicio y los responsables del mismo, el costo del plan, manejo del riesgo residual.
		RISK:SG5.SP2	**Implementar estrategias de Riesgo** La organización toma una posición frente a los riesgos, y se espera que las estrategias que establece en la gestión de riesgos se sigan durante el todo el proceso, es por esto que los planes y estrategias de mitigación de riesgos serán implementados y además monitorizados. Lo que se gana con este ciclo continuo es que en un entorno cambiante de riesgos, debido a las nuevas condiciones de complejidad que se ve en las organizaciones de hoy en día, se tenga claro que la estrategia esté bien dirigida y los riesgos bien identificados, y en caso de cambios se revise y se modifique. El producto de esta práctica será la documentación de la implementación del plan de mitigación, y una visión actualizada del estado de los riesgos de acuerdo a la

			efectividad de la mitigación frente a las condiciones actuales, a través de la monitorización y unas políticas de seguimiento.
	RISK:SG6	**RISK:SG6.SP1**	**Revisar y ajustar estrategias para proteger los activos y servicios** Una de las formas de gestionar el riesgo operacional es la protección de activos y servicios, por lo tanto los controles que se implementen con este fin deben ser evaluados constantemente y actualizados según se requiera con base en la información que proporcione el riesgo. Los controles serán el resultado del proceso de gestión de riesgo o de los requisitos de resiliencia, la experiencia de la organización es la que le dará la madurez de la definición de estos controles, mejorar los actuales e implementar los que necesite, así como la consideración de controles que podrán proteger los activos y servicios de situaciones de riesgo emergentes. El producto de esta práctica será la lista de controles a revisar, mejorar o desarrollar y un plan de revisión.
		RISK:SG6.SP2	**Revisar y ajustar estrategias para sostener los servicios** La otra forma de gestionar el riesgo operacional es el sostenimiento de servicios, por lo tanto las estrategias de continuidad del servicio serán fundamentales de acuerdo al análisis que se realice en caso que el riesgo se materialice. Para esto se plantean planes de continuidad del servicio. Basado en la información de riesgo y lo aprendido en el ciclo de vida del riesgo, se pueden identificar falencias en la definición de los planes a través de las revisiones y posteriormente proponer mejoras. La validación de los planes será una manera de saber su efectividad frente a riesgos o amenazas operacionales El producto de esta práctica será la lista de planes de continuidad del servicio a revisar, mejorar o desarrollar y un plan de revisión.
RDD	**RRD:SG1**	**RRD:SG1.SP1**	**Establecer Requisitos de Resiliencia Empresarial** La organización a nivel de empresa, debe definir los requisitos de resiliencia con base a lo que necesite, generalmente motivados por la estrategia o cuestiones de cumplimiento. Debido a que el software es un activo de tipo “tecnología”, los requisitos que se tendrán en cuenta son los que están ligados a la integridad y disponibilidad, si hace parte de un grupo de activos podrá también considerarse la confidencialidad. Como producto de esta práctica tenemos la lista de requisitos de resiliencia que define la empresa, que son el producto de la estrategia, objetivos, leyes, reglas y políticas, y serán suministrados al equipo que decida la contratación de una solución cloud como parte de la decisión.
	RRD:SG2	**RRD:SG2.SP1**	**Establecer Requisitos de Resiliencia de Activos** Una vez teniendo conciencia de los requisitos de empresa con los que se verá afectado el software, se tendrá que tener en cuenta como tal los requisitos de resiliencia que conciernen directamente al software. Es claro que estos requisitos se definirán con base en los servicios de alto valor que desee proteger y sostener la organización y por ende al activo que lo soporte, que para este caso es el software. Por tanto en esta práctica se deberá hacer una lista de lo que se considera en la organización como servicio de alto valor, establecer las relaciones entre servicios, procesos de negocio y para este caso específico el software asociado, y la lista de requisitos de resiliencia por cada software de la organización que esté asociado con un servicio de alto valor. Ya que hablamos de software, es importante que se realice una buena práctica para la ingeniería de requisitos, de modo que el software que se contrate cumpla con los requisitos que la organización establece y que mantenga la resiliencia operacional de la organización. Teniendo ya asociados unos propietarios (proceso ADM) y con buena parte de la evaluación de riesgos (RISK), esta identificación tiene una entrada de información significativa
		RRD:SG2.SP2	**Asignar Requisitos de Resiliencia Empresarial a los Servicios** Los requisitos de resiliencia que afectan los servicios deberán ser asignados a los servicios. Aquí se establecerá la relación necesaria para identificar la colección de requisitos de resiliencia para los servicios, a través de la asociación entre misión de empresa-misión de servicio-activo asociado. El producto de esta práctica es asociada a la lista de RRD:SG1.SP1y RRD:SG1.SP2 y tendrá en cuenta los servicios relevantes junto con los requisitos de resiliencia específicos por servicio. Con esto se identifica y asignan los requisitos aplicables bajo la relación requisito empresa -requisito de servicio-requisito de activo. Esto será de gran ayuda para establecer la relación del activo software con los requisitos de los servicios y la estrategia de resiliencia operacional de la organización.

	RRD:SG3	**RRD:SG3.SP1**	**Establecer una definición de la funcionalidad requerida** La organización debe tener definidas las funcionalidades requeridas de un activo en el contexto del servicio, por lo tanto es tener clara la funcionalidad que el software va a proporcionarle al servicio de la organización y cómo se va a mantener el software a través del ciclo de vida. Realizar una monitorización de esto proporciona una entrada para el análisis y validación de los requisitos de resiliencia a nivel de activo. Esta hace parte de la descripción del activo que se hará en ADM y estará documentada.
		RRD:SG3.SP2	**Analizar Requisitos de Resiliencia** Es claro que los requisitos de resiliencia buscan proteger y sostener los servicios, sin embargo también es de resaltar que en una organización hay requisitos que dependen de otros requisitos, o que tal vez un requisito entre en conflicto con otro que es prioritario. Lo que busca esta meta es que se analicen los conflictos que hay en los requisitos, si hay conflictos realizar planes de mitigación a los conflictos, y esto hacerlo a nivel de los activos, en este caso software. La definición de funcionalidad junto con el análisis de requisitos a nivel de activos nos puede dar una idea de los conflictos, y con base a esto se pueden hacer los ajustes necesarios y desarrollar los planes de mitigación para resolver los conflictos. Estas definiciones ayudarán al entendimiento de cómo el software contratado afectará los requisitos de resiliencia de empresa y de otros activos, entre ellos otras aplicaciones de la organización. Esto deberá tenerse en cuenta en el proceso de contrato del software.
		RRD:SG3.SP3	**Validar Requisitos de Resiliencia** Teniendo una consistencia en los requisitos de resiliencia a nivel de activo, podemos decir que cumple con las expectativas de protección y sostenimiento que se necesitan, y si se asegura a este nivel, tendremos resiliencia en los servicios y en la operación de la organización. Con lo que proporciona RISK, tenemos que asegurarnos que hay requisitos de protección y sostenimiento tanto para el software como para su proceso de estudio y contrato. Del mismo modo, esta práctica busca optimizar los requisitos realizando una revisión en la que se detectarán los vacíos y con esto las actualizaciones o mejoras en los requisitos y en las medidas a implantar. De este modo, esta práctica proporciona un análisis entre objetivos estratégicos y requisitos de activos y un análisis de requisitos para asegurarse de qué se necesita para proteger y sostener el activo en relación con el servicio.
RMM	**RRM:SG1**	**RRM:SG1.SP1**	**Obtener un entendimiento de los Requisitos de Resiliencia** En el área de proceso RRD ya se establecen y definen los requisitos, de modo que ahora se deben entender, es decir que todos los propietarios de los servicios y los vigilantes y propietarios de los activos entiendan su rol y responsabilidad dentro de la implantación de la resiliencia en la organización. Para esto el área de proceso ADM tendrá un papel muy importante. Como se indicó anteriormente, en gran parte el propietario del activo tendrá que definir cuáles son los requisitos de resiliencia, en este caso el software. Esto lo hará basado en el entendimiento de la motivación de la organización y la búsqueda de la protección y sostenimiento del activo. Del mismo modo tendrá que tener en cuenta los requisitos de empresa y los análisis de la evaluación e impacto de los riesgos. Como producto de esta práctica tendremos los criterios de evaluación y aceptación de los requisitos por los vigilantes, y un acuerdo entre los propietarios y vigilantes del activo de mantener el conjunto de requisitos establecidos.
		RRM:SG1.SP2	**Obtener un compromiso con los Requisitos de Resiliencia** Es necesario que además de entender, haya un compromiso para la implementación de los requisitos establecidos. En esta práctica es significativo que la comunicación a los vigilantes, pues ellos estarán en contacto permanente y podrán entender lo que necesitan asegurar para el activo, por lo tanto se les debe comunicar lo que necesitan saber y que ellos hagan ese compromiso de implantar y mejorar los requisitos. Los propietarios serán los encargados de monitorizar y mejorar lo que suceda durante el ciclo de vida del activo. Como producto de esta práctica tenemos los compromisos documentados de requisitos y cambios en los requisitos, esto puede estar, por ejemplo en el acuerdo de nivel de servicio SLA.
		RRM:SG1.SP3	**Gestionar los cambios en los Requisitos de Resiliencia** La práctica anterior pide que se documente los compromisos en los cambios de los requisitos, esta práctica establece que haya un proceso definido de gestión para esos cambios. Es claro que las condiciones actuales de las organizaciones hacen que los escenarios de riesgo cambien y así mismo los requisitos de resiliencia, es por eso que se debe establecer este proceso que dicte los lineamientos para identificar y gestionar cambios. Se recomienda alinear la gestión del cambio con el marco que se implemente en la gestión de servicio de TI, bien sea ITIL o ISO 20000, y del mismo modo establecer

			los responsables y aprobadores de cambios. Como producto de esta práctica tendremos la base, el estatus, la base de datos –incluyendo historial de cambios, los criterios de cambio y peticiones de cambio de los requisitos.
		RRM:SG1.SP4	**Mantener la trazabilidad de los Requisitos de Resiliencia** Es importante seguir el ciclo de vida de los requisitos, su desarrollo, implementación y monitorización. La organización tiene que estar al tanto que las necesidades que tenía y que tradujo en requisitos, son satisfechas por las actividades propuestas. Es muy importante tener en cuenta el área de proceso RRD, pues teniendo claro los requisitos podemos realizar una matriz de trazabilidad y proponer un sistema para el seguimiento de los requisitos, con esto no solo conoceremos los activos que se relacionan sino con esto manejaremos los conflictos, y tendremos mucho más presente las interdependencias (Es claro que el software podrá soportar uno o más servicios de alto valor, o será parte de un grupo que soporte uno o más servicios)
		RRM:SG1.SP5	**Identificar Inconsistencias entre los Requisitos de Resiliencia y las actividades desarrolladas para satisfacer los requisitos** Realizar la trazabilidad de la práctica anterior nos puede ayudar a la identificación y gestión de las inconsistencias entre requisitos y actividades, la idea es garantizar que se cumplen los compromisos con los requisitos y las actividades a desarrollar con el fin de garantizar la implementación de la resiliencia en la organización. En algunos casos a pesar de los esfuerzos, algunos requisitos no se cumplen porque dependen de más de un activo, en este caso se debe identificar y documentar esas inconsistencias para poder realizar las acciones correctivas pertinentes. Por esta razón se sugiere hacer revisiones de consistencia entre actividades y requisitos.
CTRL	**CTRL:SG1**	**CTRL:SG1.SP1**	**Definir los objetivos de control** Los objetivos de control son una manera de evaluar el rendimiento del sistema de control interno de la organización, sirve para garantizar un nivel apropiado de controles que le ayuden conseguir los objetivos estratégicos. Se pueden establecer objetivos de control, en TI por ejemplo, para asegurarse que el software y los sistemas consiguen los objetivos de una manera segura, eficaz y eficiente con un alto grado de protección y sostenimiento de un servicio de alto valor. Un ejemplo es el uso de objetivos de control es COBIT, para la gestión de TI. Pero así como definen algo general pueden llegar a definir algo específico. Es por esto que la definición es muy importante, pues para este caso de gestión de la resiliencia operacional, específicamente la resiliencia del software, los objetivos de control se definen en relación con los objetivos estratégicos de la organización, la información adquirida en RISK y en RRD. Los objetivos de control apuntarán a las estrategias de protección y sostenimiento de los activos relacionados con los servicios para asegurarse de que se gestiona su exposición a vulnerabilidades y amenazas. Con base en estos objetivos de control y las estrategias de protección y sostenimiento, se seleccionarán, analizarán y gestionarán los controles específicos. Como producto de esta práctica tendremos las directrices para la selección de los objetivos de control, los objetivos de control como tal, criterios para la priorización y lista de objetivos de control. Esto será importante a nivel general para establecer responsabilidades en la organización con base en los marcos de gestión como COBIT.
	CTRL:SG2	**CTRL:SG2.SP1**	**Definir los controles** Teniendo como referencia los objetivos de control y las estrategias de protección y sostenimiento de los servicios y activos de alto valor, se definirán los controles. Los controles no son necesariamente tecnológicos (Usando prácticas de *Secure Coding* nos ayuda a asegurar el producto, no necesariamente el proceso de implantación o entrega). Un control será una política, procedimiento, método, metodología, tecnología o herramienta que satisface un objetivo de control. Los controles que interesan a la gestión de resiliencia operacional son los que reducen la exposición a amenazas o vulnerabilidades que afectan a los activos y de este modo a los servicios y que ayudan a que esos mismos servicios y activos respondan y se recuperen mientras están en estado de interrupción. Estos controles podrán ser administrativos, técnicos o físicos a nivel general, y por su naturaleza preventivos (Separación de responsabilidades, documentación adecuada,…), detectivos (monitorización, auditorías,..), compensativos o correctivos. La práctica de esta parte es el listado de controles que protegen los servicios y activos. Controles a nivel de empresa, controles a nivel de servicio y activo y una matriz entre objetivos de control y controles (como la que ofrece COBIT). Del mismo modo asignar responsables para su implementación. Como estamos hablando específicamente de software, los controles específicos de producto son los que se implementen en el proceso TM.
	CTRL:SG3	**CTRL:SG3.SP1**	**Analizar los controles** Como una práctica ya conocida, es necesario realizar el análisis de los controles existentes, de modo que los controles concuerden con los requisitos de resiliencia y ayuden al logro de los objetivos de control. Adicionalmente es una oportunidad de considerar más controles,

			Como resultado de esta práctica encontramos el análisis de resultados, los objetivos que se satisfacen por los controles, vacíos en los controles, mejoras necesarias, controles propuestos, riesgos relacionados con objetivos de control no cubiertos y riesgos relacionados con riesgos redundantes y/o conflictivos
	CTRL:SG4	**CTRL:SG4.SP1**	**Evaluar los controles** Una vez hecho el análisis, es preciso evaluar si los controles satisfacen los requisitos de resiliencia establecidos. Esta es una manera de medir la efectividad de los controles de acuerdo a la iniciativa de resiliencia que tiene la organización. Esta evaluación debe hacerse de manera periódica, para poder mantener la gestión de los objetivos de control que estén orientados a la protección y sostenimiento de los servicios. El producto de esta práctica será la evaluación de los controles que contará con un alcance, unos resultados, áreas de problema, mejoras o actualizaciones a los controles existentes, nuevos controles propuestos, planes de remedio, actualizaciones a los planes de continuidad y riesgos relacionados a problemas sin resolver.
SC	**SC:SG1**	**SC:SG1.SP1**	**Planear la continuidad del servicio** En la tarea de proteger y sostener los activos, específicamente el sostenimiento dependerá de una estrategia efectiva de la continuidad del servicio. La organización debe enmarcar una estrategia de continuidad del negocio, y esta orientará la estrategia de la continuidad del servicio y su gestión para los procesos destinados a la planeación y ejecución de la sostenibilidad. LA idea es garantizar que los servicios de alto valor alcanzan la misión del servicio a pesar de situaciones de estrés y/o interrupción. Como primera medida se deberá elaborar el plan de continuidad del servicio para su desarrollo e implementación en los procesos de continuidad de servicio de la organización. La planeación mostrará el cómo la organización va a manejar la continuidad del servicio, y esto será una de las bases de la resiliencia operacional. El producto de esta práctica será el plan para la gestión de la continuidad del servicio –donde deberá estar alineado con: la posición de la organización frente a la continuidad del servicio; con la estructura del programa y los procesos de continuidad del servicio; con los requisitos relativos a la gestión de la resiliencia operacional del programa de continuidad del servicio; con los medios y las actividades relacionadas con la identificación y priorización de los servicios y activos para la continuidad; con las funciones y responsabilidades necesarias para llevar a cabo el plan y el programa; con las necesidades y requisitos de formación aplicables; con los recursos que serán necesarios para cumplir con los objetivos del plan; con los costos y presupuestos relevantes asociados a la continuidad del servicio. Y como es fundamental las peticiones de compromiso y el compromiso como tal que se haga con el plan deben estar documentados.
		SC:SG1.SP2	**Establecer estándares y directrices para la continuidad del servicio** Debido a la importancia de la continuidad del servicio, no se debe dejar de lado la implementación de mejores prácticas y aprender de los casos de éxito, por esto es necesario establecer y comunicar los estándares y directrices para la continuidad del servicio. Esto debe estar orientado a los objetivos de la organización. El producto serán las normas y directrices para la gestión de la continuidad del servicio. Estos serán desarrollados y comunicados resaltando responsabilidades, requisitos, entregas documentadas, modelo del contenido del plan, prueba de requisitos, y lo que se considere necesario para dejar claro el plan.
	SC:SG2	**SC:SG2.SP1**	**Identificar los servicios de alto valor para la organización** Para saber cuáles son los servicios a considerar, es necesario identificar y priorizar aquellos que son de alto valor, es decir aquellos que se requieren para que se cumpla la misión de la organización. Identificando estos servicios, será posible identificar el alcance y el tipo de plan de continuidad del servicio que se debe desarrollar e implementar. La idea es identificar los servicios de alto valor para la organización y sus activos asociados, esto puede basarse en lo que se defina en ADM En un marco de gestión de TI es claro que se tendrá claro cuáles son los objetivos de la empresa que se ven soportados por un servicio y que a su vez será un servicio de alto valor apoyado por un activo software. El resultado es la priorización de los servicios, actividades y activos asociados de alto valor (Apoyado por ADM). Igualmente los resultados de la evaluación de los riesgos en seguridad (Apoyado por RISK) y análisis de impacto en el negocio.
		SC:SG2.SP2	**Identificar dependencias e interdependencias internas y externas** Es claro que con el aumento de complejidad en las relaciones de las organizaciones, la resiliencia operacional cambia, por eso es importante para identificar y analizar las dependencias internas y externas y las interdependencias con el fin de asegurar la continuidad de servicio. En el caso de estudio deberá dejarse claras las responsabilidades de terceros sobre los servicios de la organización, manejar las relaciones y establecer responsabilidades. Como producto tendremos los proveedores de servicio de los cuales se depende, la lista de entidades externas que están incluidas en la entrega del servicio. El proceso ADM nos ayudará a identificar el activo que dependa de manera externa y la gestión con el área de proceso EXD.

		SC:SG2.SP3	**Identificar los registros y bases de datos organizacionales vitales** Una de los aspectos más importantes para la organización, y que está recogido en otra área de proceso CERT-RMM (*Knowledge and Information Management*) y que no tendremos en cuenta para esta guía es la resiliencia de la información. Para la organización la información es de vital importancia y mucho más si contribuye a los aspectos de la resiliencia operacional. Es por esto que se debe identificar la información vital requerida para la continuidad del servicio. Por lo tanto se deberán identificar y documentar los registros y bases de datos vitales, el personal fundamental y sus funciones específicas en el aprovisionamiento de los servicios, y asegurarse que los registros y bases de datos sean protegidos, accesibles y usables si ocurre una interrupción. A pesar que no concierne directamente a una medida a implementar en el software, si es una realidad que la información será importante en los sistemas resilientes.
	SC:SG3	**SC:SG3.SP1**	**Identificar los planes a ser desarrollados** Una vez establecido, se debe identificar cuáles son los planes de continuidad de servicio requeridos y que serán desarrollados, probados, ejecutados y mantenidos. Este deberá tenerse en cuenta durante el diseño e implementación de requisitos de resiliencia sobre los servicios y activos, es decir que para el software será importante que se tenga un trabajo paralelo en cuanto al plan y el soporte de los servicios o servicio al que vaya a soportar. Igualmente en este estará el resultado de las evaluaciones de riesgos en seguridad, las estimaciones del impacto, los requisitos de cumplimiento y considerando los Black Swan y las catástrofes.
		SC:SG3.SP2	**Desarrollar y documentar los planes de continuidad del servicio** Una vez identificados, se deben desarrollar y documentar los planes requeridos para la continuidad del servicio. Este se deberá realizar con base a los estándares y lineamientos establecidos. El software toma relevancia porque el personal de TI se involucra de manera significativa en el desarrollo y documentación del plan, en especial por los servicios que son automatizados o tienen una o más aplicaciones asociadas. Con el personal de TI y los propietarios del servicio en el equipo que elaborará los planes de continuidad, la resiliencia en el software será decisiva no solo por un servicio software directamente sino por otro tipo de servicios que puede soportar. Esta práctica nos dará como resultado las plantillas de los planes y los planes como tal para la continuidad del servicio. Dentro de esto deben recogerse los aspectos claves (p. ej. Actividades alternativas a desarrollar, recursos alternativos, activos de alto valor necesarios para soportar el plan), responsables e interesados.(Sobre todo si se implican terceros tener presente EXD), y cuestiones legales y de cumplimiento (p.ej. preparación frente a amenazas naturales o terrorismo)
		SC:SG3.SP3	**Asignar personal a los planes de continuidad del servicio** Para tener la certeza que el plan se ejecutará de manera eficaz, es necesario asignar miembros del personal a los planes de continuidad del servicio Al asignar personal, se deberá escoger personal que tenga las habilidades y responsabilidad de responder durante la ejecución del plan. Dependiendo del caso el personal será interno o externo (dependerá de contrato y SLA). Como producto de esta práctica tendremos los requisitos de personal a involucrar en el plan de continuidad del servicio, y la lista de miembros potenciales del personal. Una vez con esto queda asignar tareas al personal relacionado y establecer compromisos con las personas designadas. La organización se encargará también de la concienciación y formación del equipo.
		SC:SG3.SP4	**Almacenar y asegurar los planes de continuidad del servicio** Los planes de continuidad del servicio deben ser almacenados y accesibles a aquellos que lo necesiten, del mismo tienen que protegerse a través de controles de acceso que asegure que será accedido solo por aquel que sea autorizado
		SC:SG3.SP5	**Desarrollar el plan de formación para la continuidad del servicio** Para que un plan o una política tengan efecto en la organización hay que capacitar al personal, no solo del equipo sino general. Por lo tanto hay que desarrollar y administrar el entrenamiento en el plan de continuidad del servicio. Es importante que todos los involucrados en el plan tengan claras sus funciones y las responsabilidades que les competen. En algunos casos sirve para detectar vacíos de responsabilidad o habilidad en el personal. De esta práctica tendremos la lista de necesidades y vacíos del personal, una estrategia, unos materiales, unos registros y una retroalimentación de la evaluación de entrenamiento en el plan.
	SC:SG4	**SC:SG4.SP1**	**Validar los planes con requisitos y estándares** El fin de revisar el plan es que se satisfagan los requisitos y las necesidades de la organización en cuanto a resiliencia, por esta razón se tendrán que revisar los planes. Los planes de continuidad del servicio deben ser validados de modo que se eviten conflictos en el plan, que se compruebe que está alineado con lo que define la organización (estándares y directrices) y que se implementan los requisitos que establece RRD y RRM.

			Para esto se elabora una lista de requisitos que no se han cumplido, problemas de contenido y preocupaciones del plan, y un plan de actualizaciones y de medidas de remedio (los riesgos expuestos serán parte de RISK).
		SC:SG4.SP2	**Identificar y resolver los conflictos del plan** Debido a que hablamos de resiliencia operacional de la organización es normal que existan conflictos entre el mismo plan, debido a la cantidad de relaciones entre los activos, por esta razón se deberán identificar y resolver los conflictos, eso sí, bajo los parámetros de gestión del cambio que maneje la organización. En dado caso habrá que revisar o reescribir el plan.
	SC:SG5	**SC:SG5.SP1**	**Desarrollar programas y normas de pruebas** Lo que nos queda será probar el plan de continuidad del servicio, por lo tanto se deberá establecer e implementar un programa y unas normas para las pruebas. La organización deberá realizar estas pruebas en entornos controlados para asegurarse que el plan funciona y que cumple con su labor. Se debe establecer un programa, unas normas y unas fechas que permita saber que el software que soporta los servicios reaccionará ante las amenazas que se prevén en RISK y que se ven contempladas en RRD. Como resultado tendremos el programa y normas para los test considerando aspectos como estrategia de la organización, establecimiento de objetivos de calidad del test, nivel de involucre y compromiso de los interesados, reportes, revisión de aseguramiento de la calidad, directrices para manejar los problemas y directrices para la frecuencia
		SC:SG5.SP2	**Desarrollar y documentar planes de prueba** Una vez tenemos la referencia de los lineamientos, se desarrollaran y documentaran los planes de pruebas de continuidad del servicio. La importancia de documentar los procesos es que queda claro el guion, tanto lo que se quiere como los que participan, sus funciones, y los procedimientos. Se debe también tener en cuenta el entorno y tener muy claros los objetivos del test. Como resultado tendremos los planes para probar el plan de continuidad del servicio.
		SC:SG5.SP3	**Ejercer planes** Una vez teniendo la base, ahora tenemos que poner en marcha nuestras pruebas. Las pruebas nos arrojarán lo esperado en cuanto a eficacia, viabilidad y precisión a nivel general. Lo más importante serán los resultados de las pruebas, como forma de establecer que la organización está preparada para mantener el servicio estudiado, por eso deberán estar documentadas.
		SC:SG5.SP4	**Evaluar los resultados de las pruebas sobre el plan** Una vez hechos los test del plan de continuidad del servicio, revisaremos los resultados y los evaluaremos con el fin de encontrar mejoras y poder implantarlas. Lo esperado en estos casos es que los resultados del test sean los esperados de acuerdo a los objetivos definidos, y con la satisfacción del cumplimiento de los requisitos de entrada, pero no sucede así siempre. El producto de esta práctica serán el análisis documentado de los resultados, con los eventos no esperados y una lista de mejoras tanto al plan, y dependiendo de las circunstancias, al test.
	SC:SG6	**SC:SG6.SP1**	**Ejecutar planes** Una vez se definen los planes de continuidad del servicio y son probados, serán ejecutados y revisados. De manera inevitable los planes de continuidad del servicio se pondrán en marcha por diferentes razones. Lo que se espera es que se ejecuten como las condiciones lo requiere. Como buena práctica es que las condiciones se ejecuten en lo esperado y como lecciones aprendidas documentar la ejecución del plan.
		SC:SG6.SP2	**Medir la Efectividad del plan en operación** Después de la ejecución del plan, es necesario revisarlo post ejecución para identificar acciones correctivas que podrán ser implementadas como mejoras.
	SC:SG7	**SC:SG7.SP1**	**Establecer criterios de cambio** La ejecución real de los planes de continuidad del servicio nos dará condiciones reales en casos futuros, y aunque no es lo ideal, son lecciones aprendidas que serán aplicadas y que pueden mejorar y evitar consecuencias más graves. Por eso este proceso establece que los cambios a los planes de continuidad del servicio son identificados y gestionados. El producto de esta práctica son los criterios para hacer los cambios al plan de continuidad del servicio. Esto estará gestionado por los marcos de referencia que establezca la gestión de los cambios.
		SC:SG7.SP2	**Mantener los cambios a los planes** Al igual que se establecen los cambios, estos tienen que mantenerse bajo ciertas condiciones, y por los criterios que se establezcan. Por lo tanto de esta práctica se espera

			que sean las actualizaciones a los planes de continuidad y a la base de datos de los planes. Finalmente se buscará comunicar a la organización para que el personal esté al tanto de los cambios.
TM	**TM:SG1**	**TM:SG1.SP1**	**Priorizar los activos de tecnología** Hablar de software, para el Modelo CERT-RMM, es hablar de un activo de tipo tecnológico. La Gestión de TI que se establezca en la organización aportará en gran parte sobre todo a este proceso, teniendo en cuenta que manejará mejores prácticas para la gestión de activos de TI. Como se puede ver, la relación de las TI y los servicios pude llegar a ser significativa para la consecución de los objetivos que pone la compañía a nivel operacional. La priorización de estos activos tecnológicos es importante debido a que son recursos de gran importancia para la consecución de la misión de la organización por su soporte a la resiliencia operacional en cuanto a su contribución con los servicios. Toma importancia un activo, como el software, cuando se relaciona con activos de información, cuando lo provee un externo como servicio, si sirve para principios de redundancia, si aporta como control de la resiliencia de la organización o si hace parte de los planes que soportan la continuidad del servicio. Como resultado de esta práctica tenemos la lista de activos tecnológicos de alto valor (dentro del cual estará el software), que a su vez será suministrado por ADM y gestionado por nuestro marco de gestión de TI (Se sugiere COBIT), con esto podremos realizar de manera más eficaz la priorización y monitorización en caso de actualización
		TM:SG1.SP2	**Establecer los activos tecnológicos enfocados en la Resiliencia** Como se ha indicado, un software implementa resiliencia debido a la necesidad que tiene para la organización su funcionalidad en momentos de estrés o interrupción, pero esto quiere decir que posiblemente –y en su mayoría– soporta un servicio de alto valor para la organización –de los que estén en producción–, o ya sea que haga parte de los planes de restauración o ejecución de la continuidad del servicio. Esta práctica pretende que se identifiquen los activos de tecnología que soportan la continuidad del servicio y los planes de restauración. Con ayuda del marco de gestión de TI y el entorno de empresa que relaciona los servicios de alto valor, nos será fácil identificar los activos, y para nuestro caso el software que debe ser resiliente. Como producto de esta práctica tendremos la lista de los activos tecnológicos resilientes, y precisamente aquí se listará el software resiliente de la organización.
	TM:SG2	**TM:SG2.SP1**	**Asignar Requisitos de Resiliencia a los Activos de Tecnología** En esta práctica nos apoyaremos de lo definido en RRD, para establecer los requisitos de resiliencia a tener en cuenta por el activo, este será desde el punto de vista de gestión de la tecnología. ¿Por qué consideraremos en este paso estos requisitos?, esto es debido a que el software en sí mismo puede soportar o ser soportado por otro tipo de aplicaciones, con el fin de proteger y sostener el activo –una aplicación en sí misma puede protegerse con otra p. ej. Un sistema operativo puede necesitar de otra aplicación para su protección–. Es necesario identificar los conflictos de los requisitos y saberlos manejar. Finalmente tendremos documentados estos requisitos a tener en cuenta en el ciclo de vida del software que soporte los servicios
		TM:SG2.SP2	**Establecer e Implementar Controles** El sistema de control interno apoyará esta práctica, en cuanto a identificación e implementación de controles administrativos, técnicos y físicos que son requeridos para cumplir con los requisitos de resiliencia. Estos controles se implementarán con el fin de garantizar resiliencia operacional en los activos referentes a tecnología. Es claro que si se tiene una administración de la seguridad, como por ejemplo un SGSI basado en ISO 27001, y unos planes de continuidad, gran parte de los controles serán propuestos, pero los requisitos que nos proporcione RRD posiblemente nos harán implementar otros controles necesarios. Este punto es una motivación para establecer medidas dependiendo del tipo de software debido a que dentro de estos controles es importante establecerlos durante el diseño, construcción y adquisición como tal del software. Como producto de esta práctica tenemos identificados e implementaremos los controles administrativos (p. ej. Políticas a usuarios y de uso, Estándares de Interoperabilidad, procedimientos sobre personal…), técnicos (p. ej. Gestión del cambio y configuración, Aseguramiento de calidad de software, auditoría de software de grano fino,…) y físicos (aunque en el software será mucho más de soporte físico de operación) necesarios.
	TM:SG3	**TM:SG3.SP1**	**Identificar y evaluar los riesgos de activos de tecnología** Los activos tecnológicos estarán expuestos a riesgos, y el software igual, por esto se tendrá que identificar y evaluar los riesgos que le afectan. Esta práctica será conducida por los elementos que nos proporcione el marco de gestión de riesgos y las prácticas en RISK. Con esto podemos listar los riesgos que afectan a estos activos, en este caso el software (p.ej. riesgos de acciones intencionadas y no intencionadas que comprometen la protección, pobre implementación de controles que aseguren continuidad, pobre diseño y proceso de construcción…) y su impacto para la organización, esto se hará bajo criterios establecidos, de modo que con base a esto se

			establezca la categorización y priorización de los mismos.
		TM:SG3.SP2	**Mitigar los Riesgos Tecnológicos** Una vez identificados los riesgos a los que se ven comprometidos los activos de tecnología, es necesario establecer las medidas e implementarlas de acuerdo a la estrategia de la compañía. La idea es que el riesgo se encuentre en los niveles establecidos, y que se mitigue si se materializa a través de estrategias de protección que asegurarán el manejo del riesgo y la recuperación del activo sobre las consecuencias del impacto. Como resultado de esta práctica tendremos unos planes de mitigación junto a la lista de los responsables que van a conducir las estrategias de mitigación. Esto será monitorizado para posteriormente manejar el riesgo residual. De igual manera será soportado por el proceso RISK.
	TM:SG4	**TM:SG4.SP1**	**Controlar el acceso a los activos de tecnología** Para asegurarse que los activos de tecnología, y para nuestro caso el software, funcione de manera apropiada y con los resultados esperados es necesario gestionar su Integridad. El primer objetivo es asegurarse que el software no sea modificado, esto incluye la modificación no autorizada de código de software, sistemas, aplicaciones, sistemas operativos, herramientas y otros activos tecnológicos basados en software. La gestión de TI que implementa mejores prácticas, como COBIT –para la gestión de los activos de tecnología –, ISO 20000 o ITIL –para gestión de la configuración, gestión del cambio y gestión de la entrega–, e ISO 27001 –para controlar la seguridad (Triada CID)– podrán tener una ventaja competitiva para garantizar esto. El primer paso es controlar el acceso, esto quiere decir que existan medidas que controlen el acceso sólo a personal autorizado, y aseguren que no se hagan modificaciones conscientes e inconscientes del software. Estas medidas para el software suelen ser tecnológicas, a diferencia del hardware que implementa tanto medidas electrónicas como físicas. Hay que considerar los procedimientos que requerirán control de acceso, como modificaciones o actualizaciones, mantenimientos, conexiones a bases de datos, etc. Como producto de esta práctica tendremos que plantear políticas y procedimientos para el acceso (p.ej. Políticas para la gestión de acceso, Procesos de autorización de acceso, roles de usuario, políticas de gestión de identidades,…), implementar listas de control de acceso y herramientas necesarias de apoyo, así como una lista de miembros autorizados en la modificación del activo (relacionado con la gestión del cambio), en nuestro caso el software, logs y registros de auditoría.
		TM:SG4.SP2	**Ejecutar la gestión de la configuración** Uno de los aspectos contemplados dentro de la gestión de TI es la gestión de la configuración. Dentro de la resiliencia soporta la integridad de los activos de tecnología asegurando que pueden ser restaurados a un estado aceptable cuando sea necesario y provee un nivel de control sobre los cambios que afectan los servicios de la organización. La gestión de los servicios de TI establece los ítems de configuración, que son los elementos a gestionar, y para los cuales se realiza una gestión durante todo el ciclo de vida, desde sus fases de desarrollo, hasta su operación y mantenimiento, estableciendo controles durante su servicio. Se debe tener una atención especial con el software debido a que requieren estrictos niveles de control de la configuración, debido a la cantidad de cambios que se le realizan. El producto de esta práctica serán los procedimientos, políticas, directrices, normas y cuantos elementos crea la organización para gestionar la configuración de los activos de tecnología esto aplica tanto si el software es construido e implementado, usado o adquirido, tanto de manera interna como externa. Se sugiere el uso de ISO 20000 o ITIL, que implicará tenerlos en la Base de datos de configuración CMDB debidamente identificados y controlados –a través de logs y reportes–. Del mismo modo en esta práctica se propondrá las herramientas, técnicas y métodos que soportarán la gestión de la configuración. Esto a su vez podrá ser auditado. También se puede considerar unos planes de acción. Esta práctica será controlada por la gestión del cambio TM:SG4.SP3.
		TM:SG4.SP3	**Ejecutar la gestión y control del cambio** El software tiende a tener un comportamiento complejo debido a los modelos de madurez, los ciclos de desarrollo iterativos, requisitos emergentes, mejora de funcionalidades y demás, que lo hará estar en constante cambio durante su ciclo de vida, por lo tanto será trascendente que se gestionen los cambios. Los cambios tienen un papel importante en el software, por lo tanto tendrán que gestionarse para evaluar su impacto, ya sea económico, en el servicio que soporta, con otros activos que soporten servicios, etc. Del mismo modo, los cambios aportarán no solo a las mejoras, sino a la detección de fallos y mantenimiento, por eso una buena gestión garantiza un buen manejo alineado con los requisitos de la organización en cuanto a resiliencia. Como producto de esta práctica tenemos los puntos de referencia para suministrar a la gestión de configuración TM:SG4.SP2, pues la gestión del cambio se encarga de administrar los cambios a los elementos de configuración. Además establecerá las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para establecer los cambios, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, a las peticiones de cambio que se realicen se les debe hacer un respectivo seguimiento, el cual se almacenará en la base de datos de gestión del cambio.
		TM:SG4.SP4	**Ejecutar la gestión de la entrega**

			Para la gestión de servicios de TI, es necesario, del mismo modo como se establece la gestión de la configuración y del cambio, gestionar la entrega del activo tecnológico al entorno de producción. Para la gestión de la entrega en software es importante tener en cuenta el manejo de versiones, pero así mismo estas deben ser probadas antes de salir a producción y durante producción. En tecnología se maneja el término *Build* como una versión del activo que está listo para ser entregado en producción, en el caso del software puede ser por ejemplo una versión actualizada de un sistema de gestión que incorpora una mejora de seguridad. La entrega de los *builds* debe ser probada en un entorno para identificar situaciones que puedan comprometer otros activos, que refleje problemas de seguridad, etc. Una vez se identifique y se realicen las mejoras esperadas, de establecerá la entrega en producción. Así mismo en este proceso, los parches (que aportarán a la resiliencia en cuanto a mejorar el software en cuanto a gestión de vulnerabilidades) serán un tipo de entrega y tendrá que ser gestionado. Como producto de esta práctica se establecerán las políticas, procedimientos, metodologías y cuantos procesos crea necesario la organización, para la gestión de la entrega, por lo que se sugiere como marco de referencia el uso de ISO 20000 o ITIL. Adicionalmente, se recomienda la entrega de *Builds*, pero del mismo modo se debe establecer un plan y procedimiento para probar las entregas, documentar los resultados de las pruebas a los *Builds*, establecer las mejoras y entregar a producción. La gestión de la entrega estará relacionada con los procesos de gestión de la configuración y del cambio.
	TM:SG5	**TM:SG5.SP1**	**Ejecutar la planeación para el sostenimiento de activos de tecnología** Así como se gestiona la integridad, para los activos de tecnología que soportan servicios, o que son de alto valor tienen que asegurar su disponibilidad y funcionalidad, por lo tanto deben desarrollarse planes que ayuden a su sostenimiento. Los requisitos de resiliencia establecidos, definirán ciertos términos en cuanto a disponibilidad que se deben cumplir, tanto en condiciones del día a día, como en el caso que se presente una situación de interrupción o estrés. Para esto se definen una serie de las métricas que permitan establecer la disponibilidad que debe cumplir la tecnología y servicios relacionados, tanto en condiciones normales como en condiciones degradadas. En este proceso, para cada activo se establece el *Recovery time objectives* (RTOs), que consiste en el periodo aceptable de baja de un activo tecnológico y su servicio asociado, después de que la organización se ve comprometida por una situación que impacta su operación normal, este será incluido en los planes de continuidad (Área de Proceso SC) debido a que está ligado al servicio. También se establece un *Recovery point objectives* (RPOs) en el cual se define el punto en el cuál un activo tecnológico debe ser restaurado para permitir la recuperación de los activos y servicios asociados después de la interrupción, este será incluido en los planes de continuidad (Área de Proceso SC) en cuanto a la restauración. Como producto de esta práctica se tendrá como referente los resultados del análisis de impacto en el negocio o la evaluación de riesgos (Área de Proceso RISK) con el fin de definir el alcance de sostenimiento de los activos. Igualmente se deben definir las métricas (Esto se definirá en RRD y RRM). También de recogerán los RTOs y los RPOs y esto se tendrá en cuenta en los planes de continuidad del servicio (Área de Proceso SC).
		TM:SG5.SP2	**Gestionar el mantenimiento de los activos de tecnología** Es claro que tendremos que establecer una práctica en la que se definan y se gestionen los mantenimientos operativos de los activos de tecnología. Tal vez esto suene mucho más para el hardware, sin embargo el ciclo de vida del software contempla el mantenimiento con el fin de mejorar el software, por ejemplo la aplicación de parches para corregir una vulnerabilidad u optimizar un algoritmo (gestionado por TM:SG4.SP4.). El riesgo de este tipo de mantenimiento, es una posible acción, intencionada o no, que podrá terminar comprometiendo los requisitos de resiliencia establecidos. Por esta razón, este tipo de mantenimiento necesita procedimientos de control, autorización y acceso. Como producto de esta práctica tenemos la lista de mantenimiento regular que requieren los activos de tecnología junto con intervalo y especificaciones, aunque en el caso del software consistiría en lo que se pacte de mantenimiento en el SLA. Se deberá establecer una lista de personal autorizado para realizar las reparaciones. Se tendrá un documento de seguimiento con los mantenimientos registrados (tanto correctivo, preventivo, adaptativo o perfectivo). Se tendrán registradas las peticiones de mantenimiento. Esto deberá alinearse y estar controlado con la práctica que establece la gestión de cambios. En el caso de software es importante tener en cuenta la norma ISO/IEC 14764.
		TM:SG5.SP3	**Gestionar la capacidad de la tecnología** La gestión del servicio de TI, establece otra gestión que se debe hacer dentro de los activos de TI, y es la gestión de la capacidad. Para efectos de la guía, es importante tener en cuenta la capacidad operativa de los activos y poderla gestionar de manera adecuada esto debido a que la capacidad es una propiedad que está directamente relacionada a la disponibilidad. La planeación de la capacidad debe hacer previsiones, debido a la variabilidad que tiene la demanda del servicio (p.ej. horas pico y horas valle del servicio). En cuanto a software, la capacidad puede relacionarse con varias situaciones, por ejemplo usuarios concurrentes en una aplicación, la cantidad de peticiones que recibe, cantidad de espacio en memoria que utiliza, etc.

			El producto de esta práctica será el establecimiento de una estrategia que defina la gestión de la capacidad. Para construcción de software es importante que se defina en los requisitos de manera clara de la capacidad necesaria para el funcionamiento bajo cualquier condición. Adicionalmente se tendrá en cuenta marcos de referencia como ITIL e ISO 20000 para la gestión de la capacidad. Es recomendable hacer estimaciones y previsiones de las condiciones que cumplirá el software en cuanto a capacidad, por lo tanto es importante documentar los requisitos (previstos por RRD), y todos los procedimientos, políticas, planes, para su aseguramiento (esto puede afectar RPO y RTO). Para conocer el rendimiento de la estrategia, es importante establecer unas métricas para poder establecer planes de acción, y estos planes estarán ligados a los procesos de gestión de cambio.
		TM:SG5.SP4	**Gestionar la interoperabilidad de la tecnología** Actualmente la interoperabilidad de aplicaciones es un factor importante que se maneja en la organización, esto debido a las estructuras emergentes, virtualización e interconexión entre las empresas, y en general entre los sistemas. En el software específicamente se describe como la capacidad de diferentes aplicaciones de intercambiar los datos a través de formatos comunes, para entenderse en el mismo lenguaje. La importancia de gestionar la interoperabilidad es que es al día de hoy un importante factor que representa valor para la organización Como producto de esta práctica se establecerán los estándares seguidos para la interoperabilidad de modo que la arquitectura y diseño de la aplicación se basen en esos principios y mantengan el valor en cuanto a interoperabilidad minimizando los riesgos que esto implica (considerados por RISK). Se sugiere el uso de estándares para tener en cuenta en aspectos de diseño, desarrollo e implementación de arquitecturas interoperables, integración apropiada de sistemas (construidos, adquiridos o contratados), diseño adecuado de interfaces, manejo de "sistemas de sistemas", etc.

Tabla 20. Mapa de ruta para Software como servicio contratado basado en áreas de proceso CERT-RMM

6. CONCLUSIONES

- Es gratificante haber podido aplicar de manera profunda gran parte de la temática aportada por la materia Auditoria y Calidad del Software y Sistemas (Auditoria y Certificación de Sistemas; Validación del Software. Auditoría Física e Inspección; Fundamentos de la Gobernanza y la Gestión de Servicios de Tecnologías de la Información; Fundamentos de la Gobernanza y la Gestión de Seguridad de la TI) que junto a Gobernanza y Gestión de TI, fueron en gran parte las razones por las que escogí este Máster, y que pienso son de gran importancia en la formación de un profesional en informática.

- Escoger un tema innovador es un reto a la hora de encontrar fuentes fiables para tener un punto de partida en el trabajo, sin embargo tuve la suerte de encontrar el modelo CERT-RMM, en el cual baso la guía, con el que tuve una referencia importante y que en gran parte me contribuyó no solo en el producto sino en el aprendizaje en el área. Del mismo modo este tema es muy aplicable a futuro considerando las amenazas crecientes que genera la web. De igual manera, considero con mayor razón la importancia de los estándares debido a que sugieren prácticas con las cuáles las organizaciones, a través de las TI, no solo generan valor sino a su vez confianza cara al mercado.

- Una organización que establece una gobernanza de TI que está alineada con la gobernanza corporativa de la organización, tiene más probabilidades de aprovechar las ventajas que ofrece la tecnología para alcanzar los objetivos y la misión de la organización. La parte de gestión de TI debe estar integrada con la gobernanza corporativa de TI para que de la función de TI se obtengan beneficios a nivel operacional. Con esto la implantación de la resiliencia operacional sobre los activos de tecnología será mucho más fácil.

- Los marcos para la Gestión de Servicios de TI, y gestión de la seguridad de la información (que incluye la seguridad informática) y gestión de la continuidad del negocio (que incluye la continuidad del servicio), apoyan una estrategia de gestión

efectiva de resiliencia en la organización, y con esto se puede realizar esfuerzos conjuntos y coordinados, y con esto una reducción de costos.

- La gestión de riesgos es una práctica de gran importancia en las organizaciones, sin embargo en algunos casos se queda corta al no considerar los *Black Swan,* y puede ser muy costosa debido a la complejidad de las relaciones internas y externas de las organizaciones y los nuevos entornos de riesgos. Implantar resiliencia puede hacer menos costosa la gestión de riesgos y ambas estrategias pueden apoyarse mutuamente.

- La resiliencia operacional es una la solución para mantener los servicios operativos en caso de estrés o interrupción. Puesto que los servicios operativos de la organización dependen en gran parte de la tecnología, y muchos directamente del software, es necesario establecer mejores prácticas que ayuden a preservar y proteger al software y los servicios que soporte, frente a las amenazas cambiantes actuales de modo que el servicio siga operativo así sea de manera degradada. La experiencia en la aplicación de los principios de resiliencia operacional podrá definir cuáles serán las mejores prácticas para obtener un software resiliente.

- La visión operacional de la resiliencia en el software hace que no solo que el producto cumpla con los requisitos de resiliencia establecidos, sino que lo que implique el proceso dentro de la organización, y las relaciones que tenga con otros servicios y activos, también cumplan con la estrategia de resiliencia de la organización.

- Aplicar metodologías de desarrollo seguro es una buena práctica para hacer software resiliente, pero se deben considerar estrategias de continuidad del servicio en caso que un riesgo se materialice creando situaciones de interrupción o estrés. Un “Software seguro” no necesariamente es un software resiliente, pero todo software resiliente debe ser un “software seguro”.

- Las relaciones comerciales que se establecen con terceros debido al software, (el Software construido por externos, Software como servicio contratado, e inclusive con el Software adquirido*)* obliga a la organización a establecer medidas que comprometan a

las empresas externas con las estrategias de resiliencia, bien sea a través de contratos o acuerdos de nivel de servicio SLA.

- Implantar resiliencia en soluciones software construidas *in-house,* requieren un compromiso mayor en las actividades tanto de diseño y construcción, como de implantación y mantenimiento, sin embargo es mucho más fácil tener un control interno sobre ellas y por ende las soluciones resilientes dependerán propiamente de la organización, lo cual es una ventaja, sin embargo requiere una mayor inversión y cuidado durante el ciclo de vida del software.

- Implantar resiliencia en soluciones software construidas por terceros, está muy ligado al contrato que se haga con ellos, requiere un compromiso alto de la organización contratada en cuanto al seguimiento de los alineamientos y estrategia de la organización a nivel de resiliencia. La organización contratante debe suministrar todas las prácticas para que la contratada entienda y cumpla y a la vez soporte la estrategia de resiliencia establecida. También se debe asegurar que se siguen mejores prácticas en el ciclo de vida del software, por lo tanto es importante establecer en el contrato de servicio que se hará todo en cuanto sea posible para la construcción de software resiliente, y para que los servicios también se mantengan resilientes a nivel operacional.

- La resiliencia en soluciones de software adquirido es una tarea bastante complicada, en especial porque gran parte de esto dependerá del proceso de adquisición del software, pues el software ya tendrá unas especificaciones establecidas. La organización tendrá que evaluar las características del producto, la manera de implantación y el mantenimiento y que en todo momento se cumplan los requisitos de resiliencia.

- Establecer resiliencia en soluciones software como servicio contratado es muy factible, debido a que dejando claro los requisitos de resiliencia de la aplicación, y que se acuerde de manera concreta el SLA, la responsabilidad será en gran parte del tercero, sin embargo es un riesgo enorme por la gran dependencia que tendrá el servicio a prestar con la empresa externa. Sin embargo, una solución Cloud de calidad es flexible e implanta marcos de gestión servicios TI, seguridad y continuidad del negocio.

7. LÍNEAS FUTURAS

7.1 Implementación de la Guía

La guía propuesta, puede seguirse de la manera propuesta con el fin de cubrir todos los procesos para la implementación de la resiliencia del software que soporte los servicios de la organización. Esta guía se podría implementar en un entorno empresarial donde los servicios tengan alta dependencia del software y se desee evaluar de manera detallada como hacer una solución resiliente a partir del ciclo de vida del producto y del proceso, alineado con la estrategia de la organización. Esta guía no solo es legible para el jefe de proyecto de software, el desarrollador o el CIO, sino que da una idea a la alta dirección y stakeholders para justificar una implementación de procesos, políticas, métodos, procedimientos y técnicas que le dan una idea de la implementación de resiliencia operacional sobre el activo software. Una línea futura consiste en la implementación de la guía en un entorno real, de modo que se pueda analizar el aporte y la eficacia de aplicar estas recomendaciones para los casos citados.

Del mismo modo podría automatizarse la guía de modo que el que la utilice siga la ruta de acuerdo al software que gestione y con esto aplique las prácticas correspondientes a cada caso, y esto a su vez referencie las prácticas sugeridas y establezca las relaciones entre prácticas, teniendo en cuenta las dependencias que hay de unas con otras, los suministros y salidas de información y la información complementaria que se brindan entre áreas de proceso.

7.2 Evaluación de la madurez de la implementación de la guía

Una vez implementada la guía, otra línea futura puede ser medir la madurez de la solución en la organización. Esto nos podría dar una idea de qué tan preparada está la organización frente a situaciones de riesgo operacional, también sería una herramienta de verificación de la implementación de medidas (de protección y sostenimiento) con base a los requisitos establecidos, y saber la madurez de las medidas y en general de la solución que se ha implementado.

7.3 Aplicación de Métricas para la resiliencia de software

Dentro de las discusiones que actualmente se manejan a nivel de resiliencia en la organización, las consultoras proponen metodologías para saber qué tan resiliente es la organización, cuál es el grado de resiliencia de la organización, sin embargo son preguntas de ámbito general para saber el grado de preparación de la organización frente a una amenaza de interrupción de la actividad empresarial.

Una línea futura puede ser una métrica específica para la resiliencia de software, con esto se puede saber qué tan preparado está el software para afrontar ciertas amenazas. Como se había indicado, es casi imposible que un software sea resiliente a todos los casos, pero en un escenario se planteará un ambiente de riesgos y se podrá medir la efectividad de la protección y sostenimiento del software en condiciones de interrupción.

BIBLIOGRAFÍA

[AGUI09] Aguilera Díaz, V. (2009). *Crear software seguro como objetivo de la Dirección.* Ciclo de Charlas Técnicas ISACA-CV.

[AGUI11] Aguilera Díaz, V. (2011). *Diseño de aplicaciones web siguiendo el concepto hack-resilient.* Respuestas SIC. Internet Security Auditors.

[ALBE10] Alberts, C. Allen, J.H. Stoddard, R. (2010). *Integrated Measurement and Analysis Framework for Software Security.* Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[ALLE10] Allen, J.H. Davis, N. (2010). *Measuring Operational Resilience Using the CERT® Resilience Management Model.* Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[ALLE11] Allen, J.H. Curtis, P.D. Parker Gates, L. (2011). *Using Defined Processes as a Context for Resilience Measures*. Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[BART08] Bartol, N. Allen Hamilton, B. (2008). *DRAFT Practical Measurement Framework for Software Assurance and Information Security.* Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[BENI12] Carrillo Verdún, J. Benito Gómez, M (2012*). Apuntes de la Materia Fundamentos de la Gobernanza y la Gestión de Seguridad de la TI. Certificación de la Norma ISO 27001-2.* Máster Universitario en Ingeniería Informática. Facultad de Informática. Universidad Politécnica de Madrid.

[BS25999] BS. (2007). *BS 25999-2 Business continuity management. Specification*

[CURT11] Allen, J.H. Curtis, P.D. (2011). *Measures for Managing Operational Resilience.* Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[CEBU11] Allen, J.H. Cebula, J. (2011). *Software Engineering Institute Risk and Resilience: Considerations for Information Security Risk Assessment and Management.* CERT Program Session ID: GRC-202 Session Classification: Intermediate. RSA Conference 2011

[CRMM10] Caralli, R. A. Allen, J.H. Curtis, P.D. White, D.W. Young L.R. (2010). *CERT® Resilience Management Model, Version 1.0.* Software Engineering Institute, CERT® Program. Carnergie Mellon University.

[CARR12] Carrillo Verdún, J. (2012*). Apuntes de la Materia Gobernanza y Gestión de TI.* Máster Universitario en Ingeniería Informática. Facultad de Informática. Universidad Politécnica de Madrid.

[COBIT5] ISACA. (2012). *COBIT® 5 an ISACA® Framework (Serie de tres documentos: Un Marco de Negocio para el Gobierno y la Gestión de la Empresa, Implementación, Procesos Catalizadores).*

[GHAN11] Gandhi, R. (2011). *Software Assurance (SwA) in Education, Training & Certification Pocket Guide v2.1.* Nebraska University Center on Information Assurance (NUCIA) University of Nebraska at Omaha.

[ISO20000] ISO/IEC. (2005). *ISO/IEC 20000- 1:2005 Information technology -- Service management -- Part 1: Specification.*

[ISO20000] ISO/IEC. (2011). *ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements*

[ISO22301] ISO/IEC. (2012). *ISO 22301:2012. Societal security -- Business continuity management systems --- Requirements*

[ISO27001] ISO/IEC. (2005). *ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements.*

[ISO38500] ISO/IEC. (2008). *ISO/IEC 38500. Corporate governance of information technology.*

[ITIL3] ITIL V3 - Service Strategy

[MEIE03] Meier, J.D. Mackman, A. Vasireddy, S. Dunner, M. Escamilla, R. Murukan, A. (2003). *Improving Web Application Security. Threats and Countermeasures.* Patterns and Practices Publications. Microsoft Corporation.

[MICR10] Microsoft Corporation. (2010). *Implementación simplificada del proceso SDL de Microsoft.* Microsoft SDL, Security Development Lifecycle. Microsoft Corporation.

[SAMM03] The Open Web Application Security Project OWASP (2011). *Software Assurance Maturity Model. A guide to building security into software development. Version - 1.0.* The Open Web Application Security Project (OWASP).

ANEXOS

I. Open Web Application Security Project (OWASP)

The *Open Web Application Security Project* (OWASP) es una comunidad abierta orientada a la seguridad y confianza en las aplicaciones que propone métodos y prácticas para desarrollar, adquirir y mantener aplicaciones seguras. Cuenta con una serie de herramientas, documentos, foros y materiales de soporte abiertos y gratuitos.

Algunos de los proyectos que actualmente desarrolla OWASP Son

- OWASP *Application Security Verification Standard* (ASVS) – Es un estándar para el desarrollo de verificaciones de seguridad a nivel de aplicación.
- OWASP *Development Guide*: Guía práctica que incluye códigos de ejemplo para J2EE, ASP.NET, y PHP. Cubre una extensa gama de problemas relacionados con seguridad a nivel de aplicación.
- OWASP *Testing Guide*: Es un marco de referencia para realizar test de penetración, incluye técnicas y prácticas para probar los problemas más comunes en aplicaciones y servicios web.
- OWASP *Code Review Guide:* Es una guía para la revisión de código con el fin de evitar las prácticas inseguras en la codificación.
- OWASP ZAP *Project: El* Proyecto Zed Attack Proxy (ZAP) es una herramienta de penetración para encontrar vulnerabilidades en aplicaciones web.
- OWASP *Top Ten*: El objetivo del proyecto Top 10 es crear conciencia acerca de la seguridad de aplicaciones mediante la identificación de algunos de los riesgos más críticos que enfrentan las organizaciones
- OWASP *Software Assurance Maturity Model:* Este proyecto consta de un marco de referencia para ayudar a las organizaciones a formular y poner en práctica una estrategia para la seguridad de las aplicaciones que se adapte a los riesgos de negocio específicos que enfrenta la organización.
- *Webgoa*t - una aplicación web de naturaleza insegura creada por OWASP como una guía para las prácticas de programación segura. Esta cuenta con un tutorial y un

conjunto de diferentes lecciones para entender cómo aprovechar las vulnerabilidades con la intención aprender a código seguro con mejores prácticas.

- Entre otros.

Los principales riesgos más críticos identificados por OWASP en el 2013son:

- A1 Fallas de Inyección
- A2 Pérdida de Autenticación y Gestión de Sesiones
- A3 Secuencia de Comandos en Sitios Cruzados
- A4 Referencia Directa Insegura a Objetos
- A5 Defectuosa Configuración de
- A6 Exposición de Datos Sensibles
- A7 Falta Control de Acceso a nivel de función
- A8 Falsificación de Peticiones en Sitios Cruzados (CSRF)
- A9 Usando componentes vulnerables conocidos
- A10 Redirecciones y reenvíos no validados

En el proyecto OWASP existe un marco de referencia abierto que ayuda a las organizaciones a formular e implementar una estrategia para la seguridad del software de modo que se ajuste a los riesgos que enfrenta la organización y este es el *Software Assurance Maturity Model* (SAMM). Esta iniciativa es interesante pues considera el ámbito completo de seguridad en la organización, y puede soportar la estrategia de seguridad en cuanto al software que tenga la organización. Con SAMM [SAMM03] se pueden evaluar las prácticas de seguridad de software existentes en la organización, construir un programa balanceado para el aseguramiento de la seguridad de software, demostrar mejoras concretas al programa de aseguramiento de software, definir y medir actividades a lo largo de la organización.

SAMM es ajustable a cualquier tipo de organización, que utilice cualquier estilo de desarrollo. Además puede ser aplicado a nivel de organización y a nivel de proyecto.

SAMM fue construido en los siguientes principios:

- El comportamiento de la organización cambia de manera lenta través del tiempo: Un programa de seguridad de software exitoso debe especificar en pequeñas iteraciones

que entreguen ganancias de aseguramiento tangibles mientras que se incrementa el trabajo a través de metas de largo plazo.

- No hay una receta única que funcione para todas las organizaciones: Un Marco de referencia debe ser flexible y permitir a las organizaciones ajustarlo a sus necesidades basado en su tolerancia al riesgo y en la manera en la cual ellos construyen y usan el software.
- La guía relacionada con las actividades de seguridad debe ser prescriptiva: Todos los pasos en la construcción y evaluación en el programa de aseguramiento deben ser simples, bien definidos y medibles.

Bajo estas funciones despliega una serie de prácticas relacionadas con cada dominio que propone en SAMM. Cada actividad puede ser desarrollada con un nivel de madurez ajustable a las necesidades de la organización y a los requisitos que establezca.

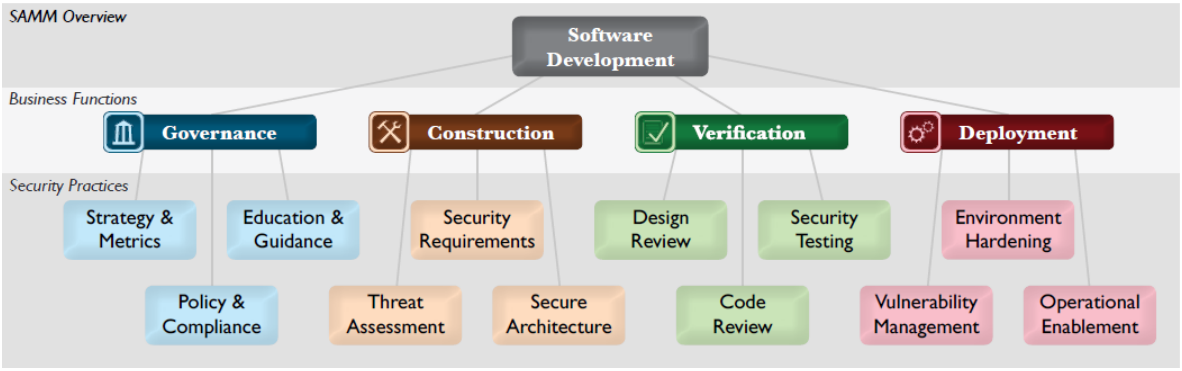

Figura I-1. Vista general de SAMM [SAMM03]

SAMM Clasifica todas las actividades en 4 dominios que representan un grupo de funciones de negocio.

- ***Gobernanza:*** Actividades relacionadas con la gestión
  - *Estrategia y Métricas:* Esta actividad propone establecer la estrategia que va a seguir la organización para la seguridad de software, del mismo modo propone establecer unas métricas que le ayuden a evaluar el valor del software y los datos la tolerancia a los riesgos que se exponen, con base a esto establecerá las prioridades de la estrategia de acuerdo a su valor.
  - *Políticas y Cumplimiento:* Esta actividad primero realiza un análisis para entender las motivaciones de la organización a nivel de gobierno y

cumplimiento, posteriormente con base a los requisitos de seguridad y cumplimiento entender los riesgos por proyecto. Luego se establecerá una comparación entre los cumplimientos y las medidas realizadas frente a las políticas y normas de la organización.

- *Educación y Guía:* La organización debe ofrecer la formación en programación y despliegue seguro al personal, así como ofrecer las herramientas y los recursos que considere para ello. Igualmente deberá formarlos en cuanto a ciclo de vida de software y responsabilidades para desarrollo seguro. En esta práctica también se incentiva a la certificación y formación integral en seguridad.

- ***Construcción:*** Orientado a la definición de objetivos y desarrollo
  - *Evaluación de Amenazas:* En esta actividad se debe identificar y entender las amenazas tanto a nivel de proyecto como de organización. Se deberá evaluar de manera continua de modo que se mejore la precisión de la evaluación y el entendimiento de las amenazas. Del mismo modo establecer controles a las amenazas tanto del software interno como externo.
  - *Requisitos de Seguridad:* En esta actividad, con base a lo que se evalúe, se establecerán los requisitos de seguridad en el proceso de ingeniería de requisitos de software. Se deberá tener en cuenta la lógica de negocio y riesgos conocidos para refinar el producto de la ingeniería de requisitos. Establecer la obligatoriedad de requisitos para software interno y externo.
  - *Arquitectura de Seguridad:* En esta actividad se pretende tener en cuenta la seguridad proactiva tanto en el diseño como la arquitectura de la aplicación. Propone dirigir el proceso a través de servicios seguros conocidos y diseños seguros por defecto. Del mismo modo, pretende controlar y validar que el proceso se realiza con componentes seguros.
- ***Verificación*:** Actividades de validación y pruebas
  - *Revisión de Diseño:* Esta actividad pretende apoyar las revisiones específicas del software con el fin de cerciorarse que se aplicaron las medidas para mitigar los riesgos conocidos, del mismo modo realizar la valoración de que el diseño aplica las mejores prácticas en seguridad y que el diseño se evalúa y valida en cuanto la aplicación de seguridad antes de pasar a codificar.

- *Revisión de Código*: Una vez el diseño se modela con los parámetros adecuados, se buscará establecer una metodología que establezca la revisión de vulnerabilidades y problemas de seguridad de alto riesgo a nivel de código. Realizar revisiones de código durante el desarrollo, se sugieren herramientas que soportan una revisión automática precisa y eficiente. La revisión ayudará a detector riesgos a nivel de lenguaje y riesgos específicos de la aplicación.
- *Pruebas de Seguridad:* Esta actividad propone establecer procesos para desarrollar pruebas de seguridad básicas basadas en los requisitos de software y la implementación. También sugieren el uso de test automáticos. En esta actividad se deberían documentar las pruebas que garanticen un despliegue exitoso en cuanto a requisitos de seguridad.

- ***Despliegue*:** Gestión del despliegue tras la creación del software
  - *Gestión de Vulnerabilidades*: En el momento del despliegue primero se deberá entender y publicar un plan de respuesta a reporte de vulnerabilidades o incidentes. Además, el proceso de respuesta debe tener unas salidas esperadas, que en caso de realizarse se pueda obtener mejoras tanto en la consistencia de las salidas como en la manera de comunicar los reportes. Este proceso hará mejorar los análisis y la recolección de datos.
  - *Fortaleza del Entorno*: En esta actividad se propone primero el entendimiento del entorno operacional del software, y con base a esto hacer lo posible para blindar el entorno para garantizar confianza en la operación de la aplicación. Esto se puede hacer a través de mejores prácticas.
  - *Habilitación Operacional*: Consiste en establecer las medidas para controlar la comunicación entre los equipos de desarrollo y operarios, de modo que sea los datos de seguridad críticos de alto interés para las partes. Al realizar la habilitación operacional, busca que se mejoren las expectativas de operación seguras y para esto se establecen unos procedimientos detallados comunicados en la organización.

II. Microsoft Software Development Life Cycle

Microsoft propone un proceso también de desarrollo del software que cuenta con unos parámetros de control de seguridad. La intención de este proceso es proporcionar una visión holística y práctica con el objetivo de reducir el número y la gravedad de las vulnerabilidades en el software. El proceso *Software Development Life Cycle* SDL introduce la seguridad y la privacidad en todas las fases del proceso de desarrollo.

Bajo esta premisa, propone tres conceptos básicos como base del proceso: formación (conciencia de cambios y amenazas), mejora continua de los procesos (comprensión causa y efecto, evaluación y mejora de procesos de SDL) y responsabilidad (entendimiento común de roles, planes de comunicación y respuesta).

"El proceso SDL de Microsoft es un conjunto de actividades de seguridad obligatorias, que se presentan en el orden en que deben llevarse a cabo y se agrupan por cada una de las fases de un ciclo de vida de desarrollo de software tradicional. Muchas de las actividades descritas aportarían ciertos beneficios en materia de seguridad si se implementaran de manera independiente. Sin embargo, la experiencia en Microsoft demuestra que las actividades de seguridad realizadas como parte de un proceso de desarrollo de software aportan mayores beneficios que las actividades implementadas de manera poco sistemática o de modo ad hoc." [MICR10]

Figura II-1. Ciclo de vida de desarrollo de software de Microsoft: simplificado [MICR10]

Este proceso pretende involucrar la seguridad en el ciclo de vida del software esperando ciertos procedimientos que la aseguren en cada fase. El proceso de mejora hará que las aplicaciones cuenten con un grado de madurez mayor en cuanto a seguridad. Los procedimientos estarán dados en cada fase considerada.

En la figura II-2, podemos ver las actividades de seguridad en un proyecto y que corresponden a cada fase identificada, desde la formación de los empleados hasta el lanzamiento de la aplicación.

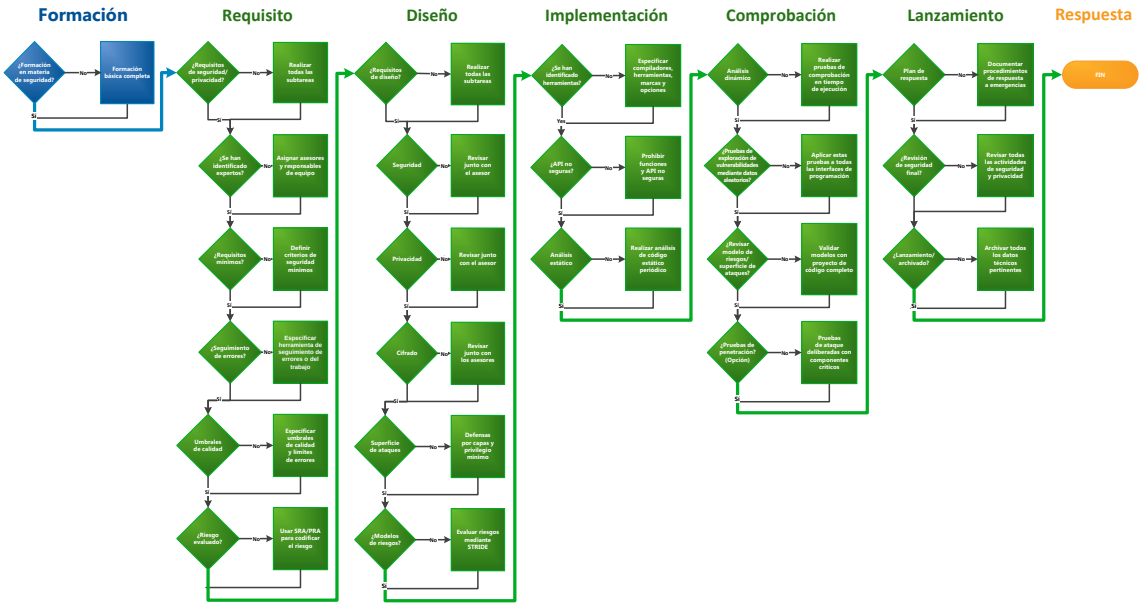

Figura II-2. Ilustración del proceso SDL [MICR10]

III. Hack-Resilient Applications

Una *Hack-Resilient Application*, es una aplicación que reduce la probabilidad de un ataque exitoso y mitiga la extensión del daño si el ataque ocurre. Es una aplicación que reside en un host seguro (servidor) de una red segura y es desarrollado usando directrices de diseño y desarrollo seguro. [MEIE03]

Uno de los antecedentes de resiliencia en el software, fue un caso real que plantea un esto debido a un caso real. El caso fue en el *Open Hack challenge* del 2002 patrocinado por eWeek, en el cual se realizaron pruebas de estas aplicaciones web *hack-resilient* basadas en ASP .NET y probadas en Microsoft® Windows® 2000. Se resistieron con éxito a más de 82.500 intentos de ataques y salió de la competencia ilesa.

Esta guía sugería que las aplicaciones web siguieran un conjunto de patrones con el fin de tener aplicaciones que protejan nuestras aplicaciones. Este concepto no solo es interesante como control protectivo para la organización, bajo este concepto asumen que hay resiliencia en el software, algo que sin embargo no es tan cierto pues a pesar de garantizar la seguridad en el software, no consideran del todo medidas para sostenimiento de la aplicación, sino un plan de mitigación del ataque.

En [AGUI11], se propone un diseño de aplicaciones con base al concepto de cuánto se debe proteger en el software, lo cuál puede ser probado con OWASP ASVS *Application Security Verification Standard*. Esta iniciativa del OWASP, ayuda a regular el cubrimiento y el nivel de rigor cuando se realiza la verificación de la seguridad de una aplicación web. La idea de la propuesta es establecer el diseño pensando en los requisitos de seguridad que requiere la aplicación.

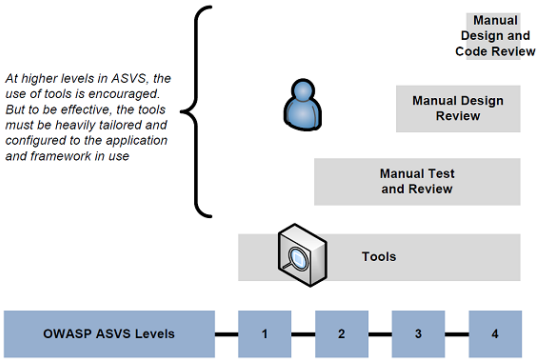

Figura III-1. Niveles OWASP ASVS[17]

Propone además unas áreas clave en la seguridad de aplicaciones, estas áreas deben tener especial atención en cuanto a requisitos de seguridad:

1. Arquitectura de seguridad
2. Autenticación
3. Gestión de sesiones
4. Control de acceso
5. Validación de entradas
6. Codificación de salida
7. Criptografía
8. Gestión de errores y logging
9. Protección de datos
10. Seguridad en la comunicación
11. Seguridad en HTTP
12. Configuración de seguridad
13. Búsqueda de código malicioso
14. Seguridad interna

[17] [https://code.google.com/p/owasp-asvs/wiki/Approach]